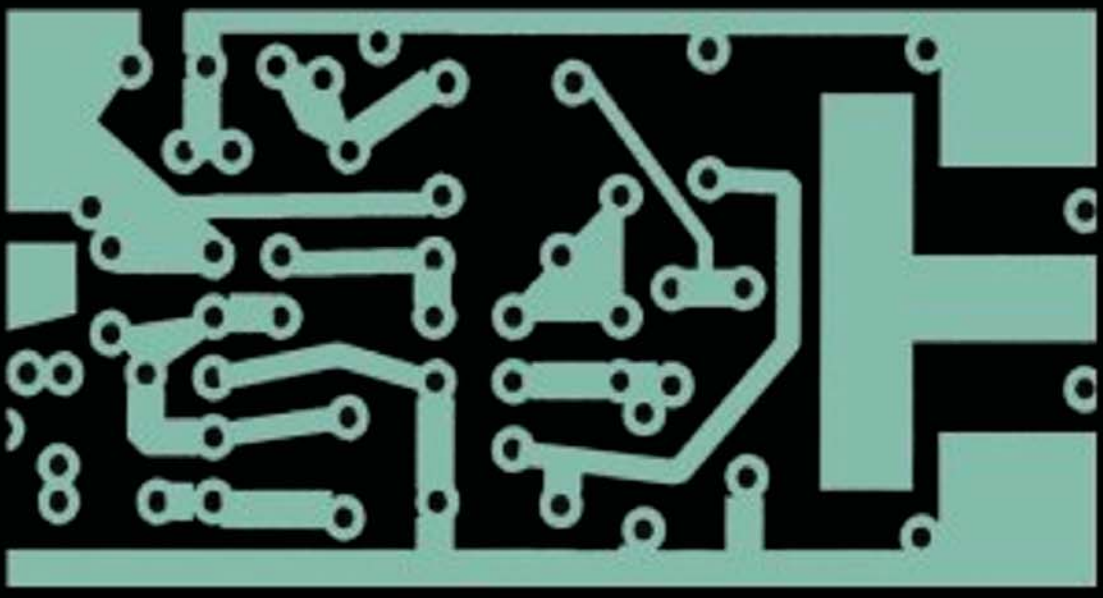
Electronic Circuits and Secrets of an Old-Fashioned Spy



Sheldon Charrett

Electronic Circuits and Secrets of an Old-Fashioned Spy

TABLE OF CONTENTS

Introduction 1
Chapter 1: Basics, Tools, and Techniques 5
Chapter 2: Reliable and Effective Room Bugs 15
Chapter 3: Building a DTMF Decoder 33
Chapter 4: Building a Red Box 57
Chapter 5: Fun and Easy: Bugs Already in Place 67
Chapter 6: Parting Thoughts 99
Appendix A: Bibliography 101
Appendix B: Legal Stuff 103
Appendix C: Contacting the Author 105
Appendix D: Files Available 107
Appendix E: Listing 1: Firmware for LCD Readout Module Interfaced with Decoder Module 109
Appendix F: Glossary 113
Appendix G: Parts Sources 115

ACKNOWLEDGMENTS

Thanks, Mom, for mistakenly believing my first book was about surveillance circuits. Great idea! And how about that lifetime of love and support? That came in handy too!

Special thanks to Kyle-the-Genius, who helped me clean the electronics lab and sat with me for hours burning PCBs and testing radio circuits. You're the bestest kid ever!

Thank you, Pauline, for listening to all of my circuit design explanations. How did you keep that smile on your face? Your support, as always, has been invaluable.

Thanks, Lisa, for encouraging me to publish my bizarre ideas and for all the years of constructive criticism and thoughtful comments. You are a true friend.

Dale, you told me something in 1990 that changed my aspirations. Remember?

Lori, your unwavering hospitality has always been appreciated.

Thanks, Dave, for the electronics manuals and for "procuring" the decoder chip (heh, heh, heh).

Thank you, Jon, for all the nice ego strokes and for taking a chance on a lunatic. Hail to her eminence, webmaster Karen, much appreciation to PR pro Tina, and gobs of gratitude to graphics guru Barb. Kudos to the rest of the gang—a real classy team.

Special thanks to Donna for helping me with the finishing touches and for making the editing process relaxing and enjoyable.

And, once again, a big triple-decker of a thank-you to Peder Lund, Paladin Press, and the First Amendment to the Constitution of the United States of America . . . thump . . . thump . . . thump—still going!

Please heed all manufacturer safety instructions when dealing with chemicals. Read and understand the instructions that come with each chemical. This includes, but is not limited to, wearing long clothing, latex or vinyl gloves, and safety goggles and working in a well-ventilated area. The information in this book is not a substitute for manufacturer guidelines pertaining to safe use of chemicals or any other tools or materials discussed herein. Do not ignore safety precautions!

If you use electronic devices to intercept conversations or gain information on parties without their consent, you are breaking federal, state, local, and international laws. Punishment for these offenses may be severe.

The author and publisher, as well as their agents, heirs, and assigns, disclaim liability for the use or misuse of the information in this book and for any injury or legal complications arising therefrom. You are operating at your own risk and peril.

INTRODUCTION

The information industry is the fastest growing industry in the United States, possibly the world. Increasingly, it seems, lenders want to check more thoroughly the credit and employment histories of their borrowers. Fiancés (and fiancées) want background checks on their future spouses. Marketing consultants want ever-increasing information on the public's buying habits. Employers want to screen potential employees, and insurance companies want a more thorough knowledge of an applicant's medical history. With the booming of the computer age, this list goes on ad nauseam.

What about two people in a relationship who wish to spy on each other? What about corporations who want to know what secret product the competition is concocting? What about the politician looking for dirt on his opponent? Thank God! is what comes to mind every time I think of these characters. You see, computer database information is all but useless in these situations, which need nothing less than a good old-fashioned spy job. In this information-run-amok age, it's refreshing to know that people still need an old-fashioned spy job from time to time. Isn't it?

In today's world of pencil pushers and computer drones, who's left to accept the responsibility of conducting a good old-fashioned spy job? Good old-fashioned spies, that's who. Unfortunately, these folks are a dying breed, and their diminishing numbers are forcing spy equipment manufacturers to cater to large police departments and FBI types. Consequently, surveillance equipment is becoming more sophisticated and more expensive. Manufacturers add new bells and whistles so that each new product subsumes its predecessor. This entices more law enforcement dollars into the manufacturers' coffers as police departments struggle to stay at the cutting edge. Alas, these new products have more sophistication than an old-fashioned spy could ever use or, for that matter, pay for. What's an old-fashioned spy to do?

Only the most self-reliant spies have managed to hang on through this technological blitz. These spies keep to themselves. They do not hire advertising agencies, marketing consultants, or public relations directors. They traipse out on their own, keep their mouths shut, do a good job, and get plenty of business by good old-fashioned word of mouth. And, most important, when they need a good old-fashioned spy gadget, they build it themselves.

There are many books on sophisticated, do-it-yourself spy gadgets and countersurveillance devices geared toward folks with a significant background in electronics. These books cover some very important surveillance techniques used by professionals in environments where bugging is the expected norm and counter-surveillance is rampant. Two of my favorites are from Paladin Press—*The Home Workshop Spy: Spookware for the Serious Hobbyist* by Nick Chiaroscuro and *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians* by Tom Larsen.

There are also several publications dealing with toy transmitters and other novelty items that pique the interest of

would-be spies and hobbyists. After brief experimentation, however, the reader soon loses interest because the devices in question are sadly limited in their capability.

There must be a happy medium . . .

This book explores some important tools used for gathering firsthand information on spouses, CEOs, politicians, and the girl next door. I'm not talking about high-tech lasers aimed at penthouse windows from two blocks away or cellular monitoring systems available only to law enforcement agencies. I'm talking about tools that are available to anybody with a sense of adventure and minimal cash flow. If you already own a programmable police scanner, you can get started without parting with any cash at all. I have included a chapter that discusses in detail some gems of surveillance devices unwittingly planted by your subject solely for your enjoyment. Just tune in! Even if you don't yet own a scanner, you'll find a couple of tricks that cost no more than a local phone call . . .

Speaking of phone calls, how'd you like to place one for free? Just turn to the chapter on red boxes. Sometimes a spy simply doesn't have the correct change to place that all-important anonymous phone call!

If you can manage to save up about $15, a trip to your local Radio Shack and some modification tips (provided by yours truly) will launch you into the realm of home-brew spy gadgets. Fun, easy, entertaining, and oh, so convenient!

And for the serious technician or strong-willed beginner . . .

Ever curious about what numbers are being dialed from your home or office when you're not around? Are you a ham radio operator who needs to know what DTMF (dual-tone multiplexed frequency) tones are being dialed on a local repeater? Maybe you've heard DTMF tones (Touch-Tone™ telephone beeps) on your scanner or radio and wished you knew what numbers were being called? If so, or if you're just a pushover for a good do-it-yourself project, you'll appreciate the chapter on building your own DTMF decoder. While you're acquiring the parts to build this project, you can read about some ingenious methods for deciphering recorded DTMF tones without a decoder.

PROJECTS COVERED IN THIS BOOK

- Etching a professional-looking PC board (PCB)
  —positive photo-resist method
  —PCB alternatives
- Building a powerful FM room bug
  —modified Radio Shack FM wireless microphone
  —SXC-49 room bug (49 MHz FET-driven FM oscillator)
- Making a reliable FM phone tap
  —modified Radio Shack wireless microphone
  —SXC-48 phone tap (48 MHz crystal-controlled FM bug)
- DTMF decoder featuring a convenient modular design
  —simple decoder module
  —binary readout module
  —seven-segment display module
  —liquid crystal display (LCD) readout with 16-digit memory module
  —decoding without a decoder (tricking the telephone company [TelCo])
- Dual-function red box for the changeless spy
  —modified Radio Shack tone dialer
- Fun and easy bugs already in place
  —locating and monitoring cordless phone frequencies
  —discovering and exploiting baby monitor frequencies
  —fun with cellular telephone frequencies
  —mapping a cellular coverage area
  —voice mail and answering machine cracking and hacking

Don't worry if you don't understand some of these topics. The function of each project will be explained in detail in the coming chapters. You will find that these methods and devices are very useful to the private detective and casual busybody alike. And for the old-

fashioned spy, this book will prove to be an invaluable reference.

PARTS SOURCES

To build these projects, you'll need parts. Most of the parts are fairly common. The biggest exception to this rule is the 8870 DTMF decoder chip. (Please see Appendix G for information on ordering this special part.)

WARNING: PATROLS ABOUND

If you decide to build any of the experiments or use any of the methods in this book, you must understand that doing so to intercept conversations or personal information of a third party is illegal and punishable by harsh fines, lengthy imprisonment, or both.

Some experiments in this book will yield working surveillance gadgets that are, in some jurisdictions, illegal to even possess. Does this mean you must destroy the project that you've worked so hard to build? The safest answer, unfortunately, is yes.

But if you don't mind fielding some tough questions from the federal authorities who happen to catch you with one of your prize gadgets, you may wish to keep in mind the following. Each project does have at least one legitimate use: *academic study*. With some imagination, you'll surely find other legal uses for these projects, thus saving them from the big parts bin in the sky. The method used to convert any project to a legitimate use is up to you.

You must consult federal, state, and local laws to determine the legality of your alterations and intended uses (including any uses or alternative uses suggested in the coming chapters). If you are a police chief, FBI agent, or other party in possession of a court-issued warrant, you may legally possess and use these devices for the purposes granted in that warrant.

IS THIS BOOK FOR YOU?

You do not have to be a private detective or an electronics engineer to benefit from this book. This book is for anybody interested in the academic study of surveillance techniques, electronic design, or both.

You can build many of the projects in this book even if you have no prior knowledge of electronics. Chapter 1 provides some tips to help the beginner through this book and into the fascinating hobby of electronics.

Even if you have no intention of ever picking up a soldering iron or touching a diode, Chapter 5, "Fun and Easy: Bugs Already in Place," explores the fine art of making the best use of bugs already on your subject's premises (e.g., cordless phone, cellular phone, baby monitor). This chapter is a book in itself and will undoubtedly serve as an invaluable reference for anybody starting a career in the surveillance industry. So, whether you're a student, engineer, FBI agent, busybody, or old-fashioned spy, the following pages will undoubtedly contain useful information you can keep at your fingertips for years to come.

CHAPTER 1

BASICS, TOOLS, AND TECHNIQUES

It simply wouldn't be fair for the circuits and design modifications in this book to be available only to persons experienced in electronics. It also wouldn't be fair for persons with experience in electronics to buy a book filled with stuff they already know. This chapter is a compromise. It will provide only the bare-bones minimum to get the beginner through the projects in this book. It will also serve as an introduction to the tools and techniques used during project construction.

If you are electronically literate, you may still appreciate the section of this chapter dealing with PCB construction techniques. Otherwise, feel free to skip around to your heart's content.

MINIMAL BASICS

If you don't know the difference between a computer chip and a potato chip, you may be wondering how you are going to get through any of the projects in this book. Answer: you must now learn the difference between a computer chip and a potato chip. More specific to this text, you must learn the difference between a resistor and a capacitor. As you'll soon see, it's really not difficult. You must also be able to read a parts-stuffing diagram and use a soldering iron. Helpful, but not critical, is to have a general idea of how to read an electronic schematic.

What Is Electricity?

Juice, current, voltage, wattage, amperage, power—most people use these terms interchangeably to describe one elusive phenomenon: electricity. It may comfort you to know that even the most educated professors and researchers still argue about what electricity actually is. For our purposes, we will say that electricity is an invisible source of energy capable of being carried along a wire, manipulated by electronic components, and converted into other forms of energy.

Two simple examples of electricity being converted to another form of energy are a light bulb and an electric fan. A light bulb converts electricity to light, and a fan converts electricity to motion.

There are literally thousands of books describing electricity in more detail. If you are still curious, a trip to your local library should yield more than enough reading material describing what electricity is.

What Is an Electronic Schematic?

The word *schematic* comes from the word *scheme*, meaning *plan*. Thus, an electronic schematic is a visual representation, or "plan," of an electronic circuit. By looking at a schematic, the trained technician can see what the electronic circuit is supposed to accomplish. Knowing what any given circuit is supposed to accomplish greatly aids the technician when troubleshooting or assembling it.

Chances are, at some point in your life, you've seen a schematic representation of an electronic circuit such as that in Figure 1.

The arcane symbols may appear somewhat intimidating to the untrained eye. The fact is, you can get through the upcoming projects

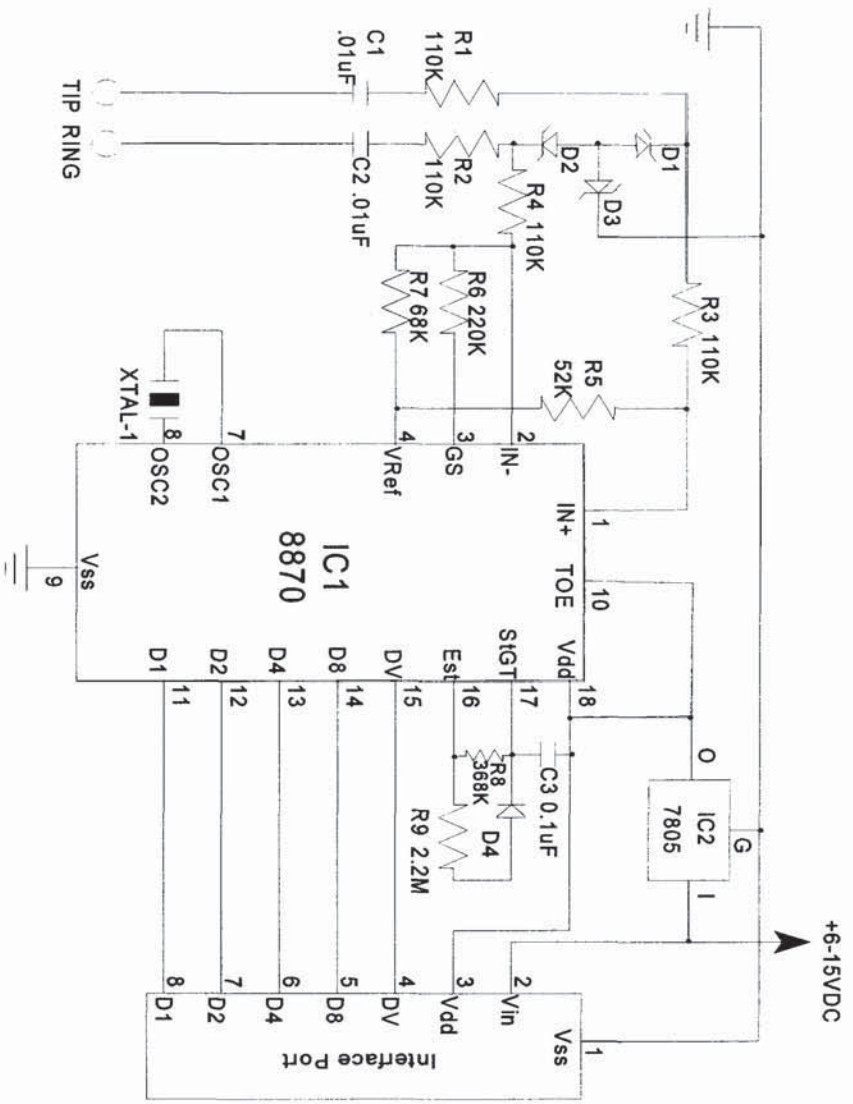


Figure 1. This is an actual schematic for a project that will appear later in this book. I hope that next time you see it, it will make more sense to you!

without knowing a thing about schematics. The PCB and parts layouts will suffice you to "get by." However, the seemingly enigmatic symbols of a schematic are actually ingenious representations of what happens to the electricity in any given circuit. The individual lines, curves, and squiggles actually do make sense. Surely, with this special knowledge in your arsenal, your projects will come together more quickly and more accurately than if you were to insert parts blindly without understanding their function. In addition, you will enjoy the reward of being able to understand what makes your circuit tick.

Basic Electronic Components

To follow the schematics and stuffing diagrams, you will need to know what a particular electronic component looks like both physically and electronically. Please refer to Figure 2 while reviewing the following descriptions.

Conductor (Wire)

The simplest schematic symbol to understand is the wire. It looks exactly like what it really is. A wire is an uninhibited path that electricity can follow.

Connection Point

A connection point is not an electronic component, but you still need to be able to recognize one on a schematic diagram. As with a wire, a connection point is also simple to understand. A connection point is represented by a dot indicating that two crossing wires are actually connected. Normally in schematics, if two wires cross paths there is no electrical connection unless there is a black dot (connection point) showing otherwise.

Switch

A switch is simply a wire that allows for temporary interruption of current flow. Its symbol is also straightforward.

Resistor

If a wire can be thought of as an uninhibited path for electricity to follow, then a resistor can be thought of as an inhibited path. A resistor is an electronic component that resists the flow of electricity, just as its schematic symbol suggests.

Resistors can have different values of resistance. Resistance is measured in ohms (often represented by the Greek omega, Ω). A 1,000-ohm resistor has more resistance than a 100-ohm resistor.

Capacitor

A capacitor acts as a storage device to hold electricity temporarily. An interesting and important characteristic of capacitors is that they do not allow direct current (DC) to pass through them. However, alternating current (AC) is capable of passing through capacitors. Capacitors, then, are perfect for isolating DC voltages from AC circuits!

The schematic symbol for a capacitor is not as obvious as some of the other symbols. I like to think of the white space between the parallel lines as a "storage tank."

Capacitors can have different values of capacitance. The unit of measurement for capacitance is the farad (F). Because a farad is a very high value, capacitors are typically measured in microfarads (one-millionth of a farad) or picofarads (one-trillionth of a farad). A 1,000-microfarad (μF) capacitor has more capacitance than a 10-μF capacitor. A 10-picofarad (pF) capacitor has more capacitance than a 5-pF capacitor.

Coil

A coil is exactly that: a coiled wire. The schematic symbol very much resembles a coiled wire.

Diode

A diode allows current to flow in only one direction.

Zener Diode

A zener diode limits the amount of voltage in a circuit.

Transistor

A transistor is very complicated and has some very special characteristics. Look in the bibliography for some good reference sources that describe transistors and their function. For now, you should know what one looks like so that you can follow the stuffing diagrams.

Battery

Knowing that most batteries are composed of multiple "cells" may help you remember its schematic symbol.

What Is a Printed Circuit Board?

Looking at a schematic of any complexity, you will note that the wire symbol runs all over the place. Wouldn't it be nice if there was some way to take care of all that wiring? That is the job of the PCB. The metal strips or "traces" on a PCB are the electrical equivalent of wires.

The alternative to using a PCB is wire wrapping. With special wire, a wire-wrapping tool, and some perforated board (often called "perf board"), you can eliminate the need to "burn" a PCB. Projects can also be assembled on a "breadboard" before actual production.

Support for the Novice

The important thing for the novice to understand is that each project is complete with a parts list, PCB layout, stuffing diagram, and step-by-step procedures. This is enough information to complete the project. The schematic diagrams will assist in wire wrapping or breadboarding. Take your time, check your work frequently, take breaks as needed, and be sure each step is completed successfully before moving on to the next. If all instructions are followed carefully, your finished work will look professional.

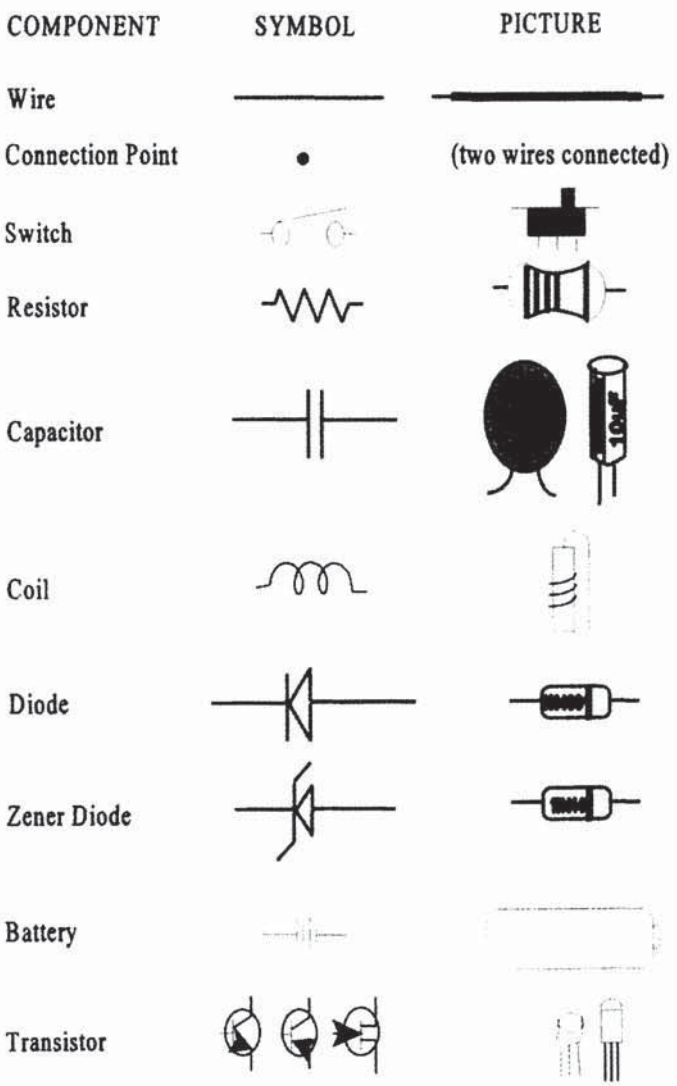


Figure 2. This chart is a quick reference for the schematic symbols used in the coming projects.

TOOLS AND TECHNIQUES

You will need some or all of the following tools during the construction of projects in this book (with the exception of Chapter 5, which is about bugs already in place):

TOOL	SOURCE	NOTES
Soldering iron (20–30 watts)	Radio Shack	
Needle-nose pliers	Radio Shack	Some pliers can also be used as cutters
Diagonal cutters	Radio Shack	
Solder sucker	Radio Shack	Optional
Solder	Radio Shack	60/40 rosin core

Radio Shack has several inexpensive kits that include all or most of the above tools plus a small stand for the soldering iron, a heat sink, and a scratching tool that is good for opening shorted PCB traces.

Multimeter	Radio Shack (for a cheap one)	Optional for testing/troubleshooting
Wire strippers	Radio Shack/used market	Optional
Drill	Check used market	
Drill press	Check used market	Highly recommended for PCBs
1/32-inch drill bit	Hardware/electronics stores	
Steel wool	Hardware store	For cleaning PCBs

Using the PCB Layouts

Each construction project in this book contains a one-sided PCB layout. Although you may use any method to transfer the layout onto a copper-clad PCB, what follows is the actual method used during the prototyping of each project: the "positive photo-resist" method. Over the years, while learning this method, I've made a thousand mistakes that resulted in as many refinements. So if you decide to use this method, be sure to follow the directions carefully. If you do, you should be able to produce a quality PCB on your first attempt.

To use this method, you will need the following:

ITEM	SUGGESTED SOURCE
Single-sided copper-clad PCB	Radio Shack, Active Electronics
Positive photo-resist spray	M.G. Chemicals catalog item #416
Developer	M.G. Chemicals catalog item #418
Ferric chloride	M.G. Chemicals catalog item #415, Radio Shack
Liquid tin (optional)	M.G. Chemicals catalog item #421
Ultraviolet lamp	Active Electronics (for exposing photo-resist)
Transparencies (8 1/2 x 11 inch)	Stationery store

As an option to the first two items, you can buy pretreated PCB from Active Electronics or another source. Ask at your local electronics store for a good source.

The procedures below may look intimidating, but this is only because the steps are broken down in detail to minimize misunderstandings. I suggest trying a small board first. If a procedure doesn't turn out quite the way it should, don't hesitate to start over and get it right. If your board doesn't come out right, take notes on what went wrong, reread the procedures, and try it again. Feel free to add your own refinements, especially with regard to photo-resist thickness, exposure time, developing time, and etching.

The instructions below represent the exact methods used to produce the PCBs during prototyping.

Procedure 1: Ensure Safety First

Heed all manufacturer's safety instructions when dealing with chemicals. Read and understand the instructions that come with each chemical. This includes (but is not limited to) wearing long clothing, latex or vinyl gloves, and safety goggles and working in a well-ventilated area. The information in this book is not a substitute for manufacturer guidelines pertaining to the safe use of chemicals or any other tools or materials discussed herein. As previously stated, the author and publisher, as well as their agents, heirs, and assigns, disclaim liability for the use or misuse of the information in this book. You are operating at your own risk and peril. Do not ignore safety precautions!

Procedure 2: Ignore Other Techniques

Unless you've had previous success with another method, ignore suggestions about PCB construction technique that you may have heard or read about.

Procedure 3: Photocopy PCB Layout onto Transparency

If you plan to use the positive photo-resist method frequently, buy a whole box of transparency sheets because it's cheaper in the long run. Otherwise, obtain a few for now.

Photocopy the PCB layout onto a transparency sheet. Be sure to keep the PCB layout centered in the copying area because photocopiers tend to distort the edges. Now, hold the transparency up to the light. How well did the toner take to the transparency sheet? You do not want to see any light filtering through the dark areas. Unfortunately, most toner-based photocopiers do not sufficiently coat the transparency film. If you can see light filtering through the blackened areas of the transparency (the PCB traces), when it comes time to expose the PCB to the ultraviolet (UV) lamp, the light from the lamp will filter through to the positive photo-resist. Upon etching the PCB you will, if you're lucky, have pitted PCB traces. If you are not lucky, you will have nothing but open traces, and your board will be useless. You will have wasted hours.

If the toner-based copier is the only type you have access to, make three transparencies of the PCB, carefully taping one over the other in perfect alignment until the traces are sufficiently dark. If the traces are sufficiently dark after overlapping two transparencies, then there is no reason to overlap the third. If you have to resort to this procedure, transparent office tape is best. Do not tape over the PCB traces because this may interfere with the UV exposure process. A small piece of tape on two opposite sides of the PCB layout will keep things aligned.

Sometimes, if you're lucky enough, you can run the one transparency through the photocopier twice and hope that everything lines up. This may help to darken the traces. But more often than not, you will make things worse. If you care to play the numbers, though, you will eventually get good alignment, which results in a usable transparency.

I've actually had much better luck with the "fax paper" type of copier. These are designed to be fax machines first, but they also allow you to make copies. The fax paper I'm talking about is the kind that comes on rolls and looks much like the now-obsolete carbon paper (not thermal fax paper). If you have access to this

type of machine, feel free to rip the PCB layout right out of the book and run it off onto a transparency. Hold the transparency up to the light. How dark are the traces? In my experience, there is a much better print, which eliminates the need for doubling up transparencies. One caveat is that some of these machines can make fuzzy copies that cause shorts on the PCB. Depending on exactly what type of machines you have access to, you may have to pick your poison.

Another alternative is to print the PCB layout right from a laser printer. Of course, this involves first having the file on your computer. The PCB layouts for this book were done on an IBM-compatible PC with Word Perfect version 6.0.

Whatever method you use, you must make sure there is no shrinkage or expansion during the photocopying process. Sometimes this is more critical than other times. For example, it is very critical that there is no size distortion when building the DTMF decoder module because you want the pins of the IC (integrated circuit) to line up with the PCB traces. A good way to test for size distortion is to first print out the PCB layout onto a plain sheet of paper. Then, insert your critical components (namely, dual inline package [DIP] ICs) into the paper PCB to make sure the holes line up with the pins. If not, you may need to enlarge or reduce the image when printing or photocopying.

Once you are sure that you have a usable transparency, move onto Procedure 4.

Procedure 4: Treat PCB with Photo-Resist

If you are using pretreated PCB, go to Procedure 5.

NOTE: Steps D through I below, as well as step A in Procedure 7, should be done in subdued light so as not to prematurely expose the photo-resist spray. A flashlight filtered with red cellophane or cloth will work fine, as will light scatter from another room.

A. Preheat oven or toaster oven to 120°F.
B. Cut a piece of single-sided copper-clad PCB slightly larger than you will need.
C. Clean the PCB with fine, oil-free steel wool.
D. Working in subdued light, spray positive photo-resist onto the PCB to the thickness of a thick coat of paint. Usually, this is not more than one or two quick squirts.
E. Use a soft artist's paintbrush (1/2 to 1 inch wide) or similar lint-free brush to spread photo-resist evenly over the PCB. Best results are achieved when brushing from the center of the PCB toward the edges.
F. Place the treated PCB in a preheated oven.
G. After 1 to 2 minutes, remove the PCB from the oven and examine the edges. Has the photo-resist spray contracted or shrunk away from the edges? If so, lower oven temperature and return to step E. If necessary, reactivate the photo-resist on the PCB by spraying a small amount of fresh photo-resist on the dried area and rebrushing. If photo-resist did not shrink away from the edges, move on to step H.
H. Leave PCB in the oven for 5 more minutes. Check it again for shrinkage. If it is okay, raise the oven temperature to 150°F and cook the PCB for 20 to 25 more minutes.
I. Remove the PCB from the oven and turn off the oven.

Procedure 5: Place Transparency on PCB

NOTE: Step A below must be performed in subdued lighting. (See Procedure 4 for definition of subdued lighting.)

A. Place the transparency on the photo-treated PCB. Make sure that the transparency is oriented properly. Because you are placing the transparency on the foil side of the PCB, traces must be oriented to the reverse of stuffing diagram traces (the stuffing diagram shows the component side of the PCB). For example, the holes and traces for a part that is to be mounted on the left side of the PCB according to the stuffing diagram should be on the right (and appear reversed) when preparing to expose the photo-treated foil side. Top-to-bottom orientation, however, should not be changed.

B. Once you are sure the transparency is oriented properly, use a small piece of tape to hold it in place and position the PCB underneath the UV lamp (which is off). Place a piece of window or picture frame glass over the PCB to press the transparency firmly against the PCB so that the UV light does not leak underneath the traces.
C. Turn the UV lamp on and expose the PCB for 7 to 8 minutes. The PCBs in this book should be no more than 4 inches from the lamp.
D. After 7 to 8 minutes, turn off the UV lamp.
E. Remove the transparency and any tape from the PCB.
F. Go immediately to Procedure 6.

Procedure 6: Develop Exposed PCB

A. In a small plastic tray (big enough for the PCB), mix one part developer to six parts warm water. You want to be sure the plastic container is big enough so that the PCB can lie flat on the bottom but not so big that you end up using more developer than you really need. Parts bin drawers work nicely for small boards (such as FM bugs). Disposable plasticware bowls also work well. For the projects in this book, 1/4- to 1/2-cup total liquid is enough. To save time, you may wish to prepare the developer while the PCB is under the UV lamp.
B. Place the exposed PCB into the developer solution and gently rock the developer tray back and forth. You will soon see a cloudy purplish material rise off the PCB. This is the exposed photo-resist breaking down and dissolving into the developer solution. Within a minute (assuming the developer is fresh) you will see the PCB pattern emerge on the board.
C. When the entire pattern is evenly visible and no more purplish clouds are rising off the PCB, the developing process is complete. A nice picture of the PCB traces should appear on the board at this time. Remove the PCB (wear your gloves and goggles!) from the developer solution and rinse it gently in cold water.
D. Move immediately to Procedure 7.

Procedure 7: Etch PCB

WARNING: Ferric chloride (etchant) is an acid. It will burn your skin, eyes, and clothes, among other things. Wear long clothing that you don't care to have ruined. Wear latex or vinyl gloves. Wear safety goggles. Follow the safety precautions on the bottle and local ordinances for proper disposal.

A. Pour an ample amount of ferric chloride into a plastic tray like the one used in Procedure 6. You may use the same tray if it has been washed thoroughly. One-fourth cup of ferric chloride is enough for a 1 x 1-inch PCB; 1/2 cup should suffice for a 3 x 3-inch PCB. Ferric chloride will work better if warmed. If warming ferric chloride on a hot plate (made specifically for that purpose), you must use a *glass* tray to hold the ferric chloride, because plastic will melt. **NOTE:** Some people have told me that the top of a toaster oven makes a good hotplate. I am not recommending this. However, if you do use this method, I suggest that you have a toaster oven dedicated to that purpose. Ferric chloride is poisonous, and you do not want to accidentally mix it with food!
B. Place the developed PCB in etchant solution for 1 minute.
C. Remove the PCB from etchant solution, rinse it off with cold water, and pat it dry with a paper towel.
D. Examine the PCB. The image on the PCB should be quite visible now and unaffected by the etchant. Areas of the PCB that were exposed to UV light in Procedure 5 should be turning a pale whitish-copper color, because they are not protected by the photo-resist and are thus interacting with etchant.
E. If there are any areas of the PCB that are etching away (turning a whitish copper color) unexpectedly, you may wish to "touch up" those areas with an indelible black magic marker. The most common problem is cracked or "open" PCB traces (usually due to gaps in the original transparency or UV light that leaked

underneath it). The black marker will prevent most of the unwanted etching.

F. Place the PCB back in the etchant and check it every 10 minutes until it is done. The etching process is completed when all the unwanted copper is removed from the PCB and only the traces remain.

G. Check for shorted traces. Remove short circuits with a sharp utility knife or X-acto knife. (See photo on page 39 for an example of shorted traces.)

Procedure 8: Drill Holes

If you got a nice print on the PCB, all your drill holes should be marked. If not, use the PCB layout to determine hole location. Drilling is best performed with a drill press and a small-diameter drill bit (1/32 inch). A small-diameter Dremel bit may be substituted, but this is slower and can get expensive if the Dremel bits keep breaking. If you don't have a drill press, you can clamp the PCB to a piece of plywood and very carefully drill the holes with a hand-held drill, though this is not the preferred method.

Procedure 9: Use Liquid Tin

This is purely optional but highly recommended. The liquid tin helps protect the copper traces from oxidation, aids solder flow, and makes your work look much more professional. The stuff is cheap, and I've found that a small amount can be reused many times (especially during prototyping).

Etching Alternatives

If it's just the photo-resist procedure that ails you, there is also an "iron-on" PCB transfer method. I've never used this technique, but feel free to check it out and let me know how it goes. Radio Shack makes a "rub-on" type of kit: catalog item #276-1577. I've tried it, but it never really grew on me. It may be useful for small projects or to someone who has a lot of patience.

Wire Wrapping

All the projects in this book can be wire wrapped. I believe Radio Shack sells a technical manual for wire-wrapping techniques. I haven't done much wire wrapping, and the little bit I did do was years ago. I do remember that it was easy . . .

Using a Soldering Iron

Even if you choose to become a wire wrapper, some of the procedures in this book still require the use of a soldering iron. Knowing how to use a soldering iron is a great skill to have. Many small household repairs are greatly facilitated by using this tool, and using it is not hard. Here are some quick tips:

1. Use a medium-wattage iron, in the range of 25 watts.
2. Use 60/40 rosin-core solder.
3. "Tin" stranded wire before soldering by heating the wire and applying a small amount of solder so that the strands become a bonded unit.
4. Make sure both parts you are soldering (such as a component lead to a PCB trace) are receiving heat from the iron. A good trick is to let the side of the soldering tip rest on the component lead and the bottom of the tip rest on the PCB. After a second or two, apply the solder to the intersection of the component lead and the PCB (not to the soldering iron!). When the drill hole is filled, remove the solder and then the iron.
5. Do not rattle the soldered joint until the solder cools down (2 to 4 seconds, depending on size).
6. Use the one-two-three-Mississippi rule. Count three Mississippis to heat the joint, apply the solder, and remove the solder and then the iron; count three more Mississippis and you're done.
7. Make sure the solder joint looks shiny. If it's dull you have a "cold solder joint," which is not acceptable. This may result from an iron that is not hot enough, movement of the solder joint before it has cooled, insufficient flux, or dirt deposits on the surface you are soldering. To remedy, clean the area, use rosin-core solder, reheat the

joint with sufficient heat, and don't jostle the connection while it's cooling.

OK, THAT'S IT!

As promised, this was a brief chapter to start the novice off on the right foot. For you advanced technicians who stuck with me up to this point, I hope you enjoyed the section on making your own PCBs. This is something that a lot of advanced electronics hobbyists still shy away from. If you are one of them, why not give it a try? It really does make a much neater finished product. It's fun too!

For you novices, just remember: there is plenty of literature out there that explores this fascinating hobby in much greater detail. If you're interested in pursuing electronics, I suggest you make a trip to your local library and check out a few books. For now, get some of the basic tools and try some of the easier projects that follow (modification of existing kits). Hands-on experience is the best education you can get. If your interest is strong, I'm sure you'll be graduating to the more advanced projects in no time.

Let's get down to business . . .

CHAPTER 2

RELIABLE AND EFFECTIVE ROOM BUGS

You may have heard that the Radio Shack Mr. Microphone and other similar devices can be used as room bugs. If you're an 8-year-old spying on your parents in a room no more than 10 feet away, Mr. Microphone and some of his colleagues, used as they're sold, may do the trick. But this group of pussyfooters has some serious drawbacks:

- Unacceptable broadcast frequency for most surveillance applications
- Poor frequency stability
- Limited input configuration
- Low output power

Let's briefly address these concerns.

Broadcast frequency: Perhaps the biggest and most obvious problem with commercial FM transmitter kits is that they are designed to broadcast in the commercial FM band. If you're spying on somebody, do you really think it's a good idea to broadcast the signal on a frequency that he is likely to pick up while channel-surfing the FM dial?

Frequency stability: Under the best conditions, frequency drift is an annoying problem. In extreme conditions, frequency drift can render these devices useless for surveillance purposes.

Input configuration: Novelty devices are designed as microphones to give users a brief thrill when they hear their voices on the radio. A microphone is supposed to be placed close to the mouth for proper functioning. This kind of microphone placement is not usually practical in the surveillance industry. In reality, a room bug needs to be sensitive to low-level conversation up to 30 feet away. It's also beneficial if the bug can be readily hooked up to a phone line.

Power output: Tandy Corporation (Radio Shack) and other major manufacturers of these devices tend to keep output power low in their effort to mollify the Federal Communications Commission (FCC).

The serious spy has limited options. He can do the following:

- Buy expensive surveillance gear (after all, you do get what you pay for)
- Modify commercially available kits to suit his needs
- Build his own room bugs

Let's examine these options.

Buying fancy gear: This really isn't a bad idea. If you have that kind of cash flow, you may wish to evaluate some of the more sophisticated surveillance devices available on today's market. The only major problem I have with this option is that it's not the subject of this book. A lesser problem is that this option can be very expensive, especially if your bug is discovered and kept by the subject. With cheaper equipment, you can plant it, leave it, and forget about it. With fancy equipment, there's always a temptation to go back and retrieve your precious device for future use.

Modifying a kit: Modifying existing kits can produce remarkable results while offering an inexpensive alternative to buying

fancy equipment and a more expeditious alternative to brewing your own. It can be fun, too! Relatively speaking, the modifications we'll be exploring are not time consuming. For these reasons, we'll kick off the project section of this chapter with some fine examples of kit modification.

Brewing your own: If it's so easy to modify commercially available kits, you may wonder what good reason could there be for brewing your own bug. Since it's unhealthy for people to be wandering around the planet wondering unnecessarily about the benefits of home-brewed FM room bugs, I'll give you a good reason—three, in fact: (1) it's a good learning experience, (2) it's fun, and (3) crystal-controlled modifications require enough effort that you're better off starting from scratch. More on this later.

MODIFICATION EXAMPLES

Radio Shack Wireless Microphone (Catalog Item # 28-4030)

This unit is an improved Mr. Microphone that is sold in kit form. The first improvement: no sledgehammer is required. The unit is not encased in a plastic cylinder, and you do not have to smash anything to get at the PCB. Assembly is not difficult. This kit would make a good first project for anybody who is learning how to use a soldering iron. I recommend building this kit according to the instructions and testing it before attempting any modifications.

POWER MODIFICATION

Experimentation with Supply Voltage (1.5 to 9 Volts DC)

Manufacturers of novelty FM microphones tend to keep the FCC happy by minimizing power output. Fortunately for us, they tend to keep their bottom line happy by not going out of their way to accomplish this. An easy power modification is to place another battery in series with the single "N" battery that Radio Shack (and the FCC) expects you to use. This will give you a nice power gain without overdriving the transistors or microphone.

You may wish to experiment with supply voltages from 1.5 to 9 VDC. You will probably find, however, that power output is not everything. If fact, there are many circumstances where it's best to keep power output just high enough to get the signal outside the premises. You can then use directional antennae or sensitive receivers to pick up the signal. You can also place a "repeater" outside the premises to retransmit the signal in a specific direction with higher output power.

Experimentation with Antenna Length

The Radio Shack wireless microphone comes with a floppy blue wire about 21 inches long. Question: Why build a 1 1/8 x 5/8-inch bug and then put a big blue beacon of a wire on it, detuned and flopping around like a warm tortilla?

The antenna is just as much a part of the circuit as the transistors, coils, and capacitors. It's amazing that so many companies take the time to design a good FM transmitter and then tell the user to "use a length of wire for the antenna." That's like saying, "Use a hunk of silicon for the transistor!" An antenna is a tuned circuit, and we must treat it as such. We're doing everything in our power to make sure a usable signal gets outside the premises. I see no reason to leave the antenna out of the mix!

A radio transmitter antenna needs to be

- impedance-matched with the oscillator's output circuit,
- resonant with the transmission wavelength,
- straight,
- vertical, and
- hidden (for our purposes).

There are several ways to satisfy all of these components. Every situation is different. What follows are some general guidelines.

Impedance matching: This should've been taken care of in the design. Antennas are low-impedance devices, and an FM oscillator is

usually designed so that its transistor bias arrangement at the output supports low impedance, or, less frequently, an impedance-matching network is built into the design.

Resonant antenna: Entire books are dedicated to this complex subject, and many "tech types" will tell you that it's simply not practical to perform antenna matching on small bug-type transmitters. This is a valid point. At these small power levels, the basic tenet is "the longer the antenna, the more output power." This is true. However, I see nothing wrong with trying to get the antenna as close as possible to some degree of resonance while we're deciding how long it should be. If the alternative advice is to "use a length of wire," an attempt at tuning our antenna certainly couldn't hurt matters.

I've conducted some brief and admittedly not overly scientific experiments and found that the advice given below, in many circumstances, does seem to improve, however slightly, transmitter performance. None of these tests found the transmitter's performance to be degraded by an antenna tuned with this method. In other words, there is nothing to lose by trying.

For a broadcast antenna to be resonant, it must be equal to some multiple of its half wavelength (**λ**/2). Since the half wavelength of our transmitter is already too big to hide (9.75 feet at 48 MHz), we will use some divisor (2, 4, 8, 16) of our wavelength. I call this method *pseudo-resonance.*

Using our 48 MHz example and assuming that we want a small antenna, let's divide our wavelength (**λ**) by 16:

9.75 ÷ 16 = 0.609375 feet
0.609375 x 12 (to convert to inches) =
7.3125 inches

Taking into consideration that 12 ÷ 16 = .75, we can simplify conversion to inches with the following formula:

Wavelength x .75 = antenna length in inches

For 48 MHz: 9.75 x .75 = 7.3125 inches

Further simplified:

351 ÷ frequency = **λ**/32 inches
For 48 MHz: 351 ÷ 48 = 7.3125 inches

Use a ruler to measure your antenna and cut it to length. For easy calculation, multiply the decimal remainder by 16 to get the nearest 1/16 inch. For example: 0.3125 x 16 = 5, so our antenna length is 7 5/16 inches. When using a spare telephone wire for an antenna, you can make a longer antenna. Keep doubling this number until you arrive at an acceptable antenna length (14.625 inches, 29.25 inches, etc.).

Straight antenna: Electrical lines of force radiate from the antenna in a parallel fashion. If the antenna is twisted in a hundred different directions, the transmitter will not radiate an efficient signal. Also, the transmitter will change frequency as the antenna flops around. For these reasons and others, it's important to use either a stiff piece of wire for the antenna or to make sure a floppy wire is held in proper position with, for instance, tape or beeswax.

Vertical antenna: Since electrical lines of force radiate parallel from the antenna, it makes more sense to have the antenna perpendicular to the Earth's surface.

Hidden antenna: Use your imagination. If you're hiding it against a white wall, use white wire. Usually it's best to keep the antenna small. With ingenious installations (e.g., inside a phone line) you can take advantage of a larger antenna.

Conversion to Carrier Current (Use as Phone Tap)

Using a single 1.5-volt battery to power the FM phone tap (illustrated later in this text) tends to produce a "carrier current" effect on the phone line, which actually works to the operative's advantage. The signal "hugs" the telephone line for a certain portion of its journey. If you're having trouble picking up the signal outside the subject's home, park your van (or whatever you're using as a listening post) next to the telephone pole nearest the residence. This should help.

FREQUENCY MODIFICATION

The resonant circuit in the Radio Shack microphone is an LC tank circuit consisting of L1 and C4. This circuit along with T1 generates the carrier frequency, which is tunable via L1 between 91 and 97 MHz.

L1 is a center-tapped inductor tunable from .27 µH to .3 µH by turning the ferrite core, which in turn changes the carrier frequency. Because this is a resonant LC circuit, any change of capacitance or inductance will change the resonant frequency. Lowering the capacitance or inductance will result in a higher frequency. Raising the capacitance or inductance will result in a lower frequency. Given that L1 is used to feed the modulated signal into the radio frequency (RF) amplifier stage, it's easier (and cheaper) to alter the value of C4. Depending on your needs and what frequencies your scanner covers, you may wish to experiment with the following values for C4:

C4 (pF)	L1 (µH)	Resulting Frequency (MHz)
47	0.27	43.93
4	0.27	91
2.2	0.27	150.14
0	0.27	445.725
47	Bead out	50.750
47	Bead in	46.560

The last two measurements on this chart were taken with the ferrite bead of L1: (a) removed from its holder and (b) screwed all the way down, respectively. The 47 pF and 2.2 pF modifications are the most stable.

To assist in your experimentation, you may wish to refer to Figure 3, which illustrates the formula for calculating the frequency of an LC tank circuit.

$$f = \frac{159{,}000}{\sqrt{LC}}$$

Figure 3. Formula for calculating the frequency of an LC tank circuit, where frequency (f) is measured in MHz, capacitance (C) in µF, and inductance (L) in microhenries (µH).

If you plug the values from the above chart into the frequency formula (remember to convert picofarads to microfarads by moving the decimal point six places to the left), you will notice that the resulting frequencies do not match up with the ones in the chart. This is due to latent capacities at the transistor junctions (which vary with frequency) and ever-present stray capacities and inductances, which become more of a factor at higher frequencies. All you really need to remember is that if you change the value of C4, the frequency also changes. You can use the above frequency formula and chart as a rough guide.

Here are some field-test measurements for the Radio Shack wireless microphone. All measurements were taken with a PRO-46 handheld scanner fitted with a Radio Shack telescoping whip antenna.

FREQUENCY	ANTENNA	PS	USABLE RANGE
43.930 MHz	0 inch	1.52 VDC	4–6 feet
43.930 MHz	2.5 inch	1.52 VDC	25–50 feet
43.930 MHz	2.5 inch	3.2 VDC	150+ feet
43.930 MHz	4.0 inch	3.2 VDC	150+ feet (with improved audio)

You may think that 150 feet is not enough to conduct effective surveillance. With a base-style receiver, a good antenna (resonance-tuned and directional), and some planning, the above values can be significantly improved. Even if you do not have access to fancy equipment, 150 feet is nothing to sneeze at. It gets the signal outside the premises. With a little imagination, any motivated operative will find a way to tune in!

You may have noticed that the test frequency I chose falls right in the cordless telephone range. You may wish to go right above or below this range when you plant a bug, but staying within the cordless range has some advantages. It's a good frequency for field-testing because exposure time is high when you're trying to take accurate measurements and notes. An accidental interception during field-testing has a good chance of being written off as an off-the-hook cordless phone picking up room audio (such as a talk show or TV show or whatever you're using to modulate the carrier). Anybody picking up the signal is probably up to no good himself, which makes a call to the FCC unlikely.

If you're wondering about the possibility of the bug's interfering with cordless phone reception (thereby prompting a call to the FCC), that is also unlikely. First, the output power of any cordless phone would dwarf the output power of this bug. Second, I chose a frequency that actually falls between legitimate cordless phone frequencies. Third, modern cordless phones have an automatic scanning feature that kicks in upon any interference.

Another nice advantage of staying in the cordless frequency range is that most scanners scan the 29-to-54 MHz band in 5 KHz steps. The 108-to-174 MHz range is scanned in 12.5 KHz steps. Since we are tracking an analog signal (which may fall in between the set frequencies of a scanner), the 5 KHz steps are more forgiving. The bandwidth of this transmitter is about 20 KHz. With 5 KHz steps, you have three or four frequencies to choose from. With 12.5 KHz steps, you may only have one.

One more interesting note: if you modify this bug to act as an FM phone tap, few people would be suspicious of picking up a phone conversation in this frequency range. The "safety in numbers" adage holds especially true here.

STABILITY MODIFICATION

Replacing low-tolerance ceramic capacitors with high-tolerance caps will help control frequency drift.

- Use 5-percent silver-mica capacitor in tank circuit (C4).
- Use 5-percent silver-mica capacitor for feedback (C3).
- Use 5-percent silver-mica capacitor for stage coupling (C6).
- Use tantalum capacitors @ C5 and C7.

Keeping the supply voltage under 4.5 VDC will keep the transistors from overheating, thereby maintaining stable oscillation.

Using a smaller, well-placed antenna is better than a longer, poorly placed antenna. Long antennas draw too much power, causing transistors to work too hard and overheat, and are more likely to cause frequency jumps as people walk by.

INPUT MODIFICATION

If you've been in the detective business for any length of time, you will have realized that life is much easier when your subject has a cordless phone. It is so convenient when you can sit down the street and fill your tape recorder with invaluable information without the worry that, at any moment, countersurveillance technicians are following a twisted pair right to your listening post.

But what if your subject does not have a cordless phone? Is there no hope for a convenient wireless listening post? Wouldn't it be nice if there were some way you could monitor a subject's phone conversations on your scanner even if he doesn't own a cordless phone? Perhaps you've even "phantasized" about anonymously sending your depraved subject a cordless phone as an "area promotion" from a new cordless phone manufacturer. Your subject could then unsuspectingly hook it up just so you could tune in. Well, it's a thought, albeit an expensive and risky one (and one I'm not recommending). A better solution to this unfortunate fact of life happens to be my favorite use for a Radio Shack wireless microphone . . .

FM PHONE TAP

An FM phone tap is the next best thing to your subject's having a cordless phone. With one of these properly planted on the premises, you'll be able to sit down the street, tune in, and pick up both sides of your subject's phone conversations.

Parts List

PART	VALUE	SOURCE	NOTES
FM mic kit	(not mike!)	Radio Shack	Catalog item # 28-4030
Transformer	8-1K audio	Radio Shack	Catalog item # 273-1380
Battery	"N" size 1.5 V	Radio Shack	Catalog item # 23-585
Battery Holder	"N" size 1.5 V	Radio Shack	Catalog item # 270-405A
C4	47 pF	JDR Microdevices	SM-47 (preferred)
Potentiometer	100K	Widely available	Can also experiment with 50–100K resistors

TOTAL COST: Less than $20

Procedure

1. Get a court-issued warrant to build and use an FM phone tap.
2. Go to Radio Shack and buy the parts.
3. Build and test an FM wireless microphone kit per Tandy's instructions.
4. Desolder C4* and put it aside for reuse later.
5. Place a 47 pF capacitor (preferably silver-mica) at location C4.
6. Desolder and remove the electret condenser microphone from the PCB.
7. Solder the black wire of the transformer to the ground side of the FM mic PCB (use the hole left by the removed condenser mic).
8. Connect the green wire of the transformer to the middle of the 100K potentiometer.

9. Connect one of the remaining terminals of the potentiometer to the "hot" side of the FM mic (use the hole left by the removed condenser mic).
10. Remember that you must supply your own 1.5-volt "N" battery! The unit does not run off a phone line. This is not an oversight. Units that draw power from the phone line are more susceptible to countermeasures.

* The Radio Shack kit used during prototyping had this part labeled as C4. The copyright date on the kit is 1994. I cannot guarantee that future versions will be labeled the same. Find the capacitor in the LC tank circuit. It is the one in parallel with the tunable coil (L1 in this example).

You now have an FM phone tap ready to be installed on your subject's phone line. Installation is best performed outside the home or where the phone service comes into the house (sometimes in an attached garage or utility area of an apartment building). This will ensure that all telephone extensions can be monitored.

Hookup is in series with the existing phone line (tip or ring). Do not hook in parallel or you'll fry the transformer! Adjust the potentiometer for low audio distortion. Refer to Figure 4 for proper connection.

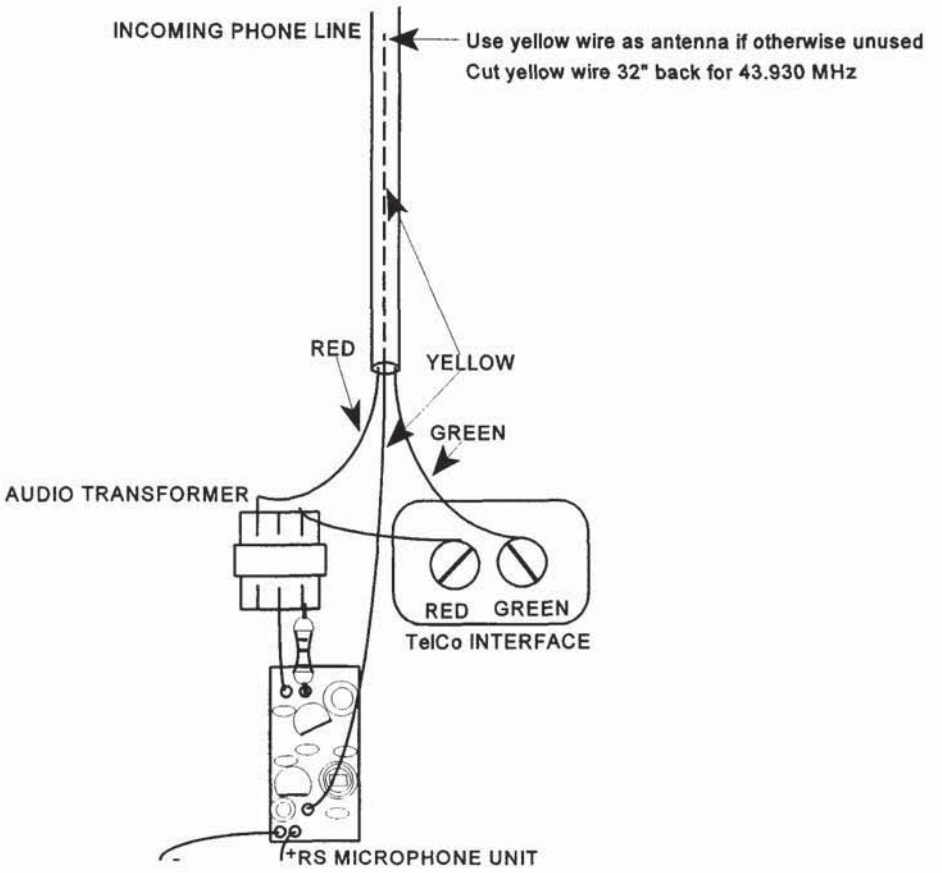
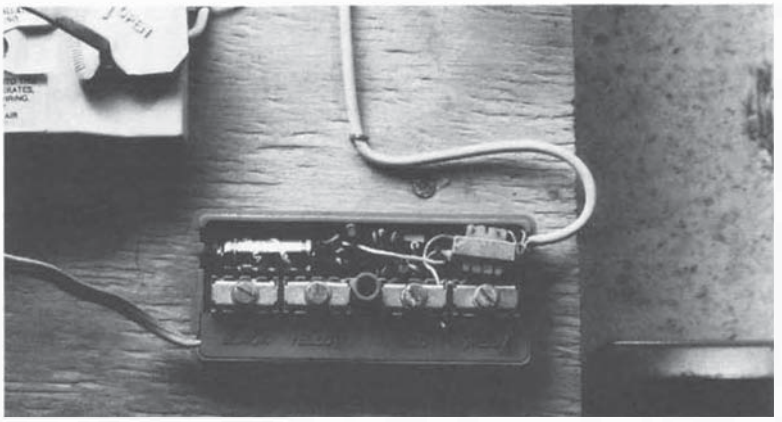
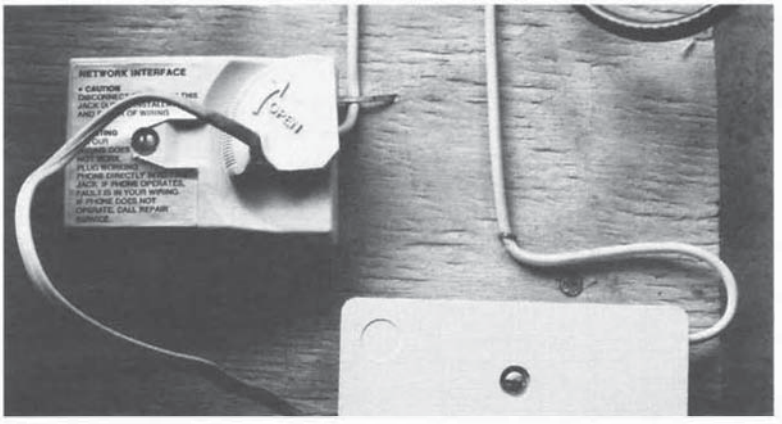


Figure 4. Use this diagram to assist in covertly planting the Radio Shack microphone in a standard TelCo interface.



Phone tap in wall. Now, what detective/author would be crazy enough to bring his camera along on a gig? If you can send two birds to their respective graves with one reasonably sized stone, why not? The cutthroat nature of this business has really driven down the pay scale on these gigs—a guy has to make the trip worth his while!



Slick and stealthy. Who would suspect that a crazy, camera-happy detective was here just moments earlier installing a phone tap? Certainly not the yuppies who own this exclusive townhouse!

Incidentally, digital/spread spectrum and voice-encrypted cordless phones can be defeated with this setup because you are not intercepting the actual cordless phone signal. You are intercepting your own radio signal, which is modulated by the analog signal from the subject's telephone line. You may wish to keep this in mind the next time you are upset that your subject has security features in his cordless phone. With the FM phone tap installed and your subject falsely secure that all conversation is scrambled, you are likely to learn his most sensitive information during these very conversations.

HOME-BREWED BUG
SXC-49 ROOM BUG
(FET-DRIVEN FM OSCILLATOR)

Here is a kick-ass transmitter that is a hybrid of several designs I've built over the years. It's designed with a 6-volt regulator, but you could replace it with an 8-, 9-, or perhaps even 12-volt regulator (with sufficient supply voltage) without compromising stability too much. The 6-volt design is nice because it can be run on one 9-volt battery. The PCB, incidentally, was designed to fit nicely on top of a 9-volt battery.

Field tests at 6 volts with a 7-inch pseudo-resonant antenna are remarkable. With my PRO-46 handheld scanner and Radio Shack whip antenna, I was able to pick up usable audio at 200 yards without having to do the funky chicken. A better receiver with an antenna tuned for 49 MHz should yield significantly increased performance. I was directed to a company that makes such an antenna. However, after writing the company two unanswered letters, I gave up on any hope of testing its product. It's cheaper to build your own antenna anyway. Again, Radio Shack has an engineering manual on how to do just that. Your local library should also have some good books on antenna construction. Since homemade antennas are not a standard that everyone can go by, I did not think it would be a good idea to report field test measurements using them.

Please note that, for reasons soon to be explained, the SXC-49 PCB also doubles as the SXC-48 PCB.

Parts List

PART	VALUE	SOURCE	NOTES
(Semiconductors)			
Q1	2N3904/2222	Radio Shack	
Q2	2N4858	Active	N-channel J-FET (other RF FETs will work well too)
U1	78L06	Widely available	
D1	SMV 1748	Active, JDR	Most varactors will
(Resistors)			
R1	4.7K	Radio Shack	Get Radio Shack package deal
R2	100K	Radio Shack	Get Radio Shack package deal
R3	22K	Radio Shack	Get Radio Shack package deal
R4	10K	Radio Shack	Get Radio Shack package deal
R5	100 ohm	Radio Shack	Get Radio Shack package deal
R6	150 ohm	Radio Shack	Get Radio Shack package deal
R7	20K	Radio Shack	Get Radio Shack package deal

Radio Shack has a few packaged assortments of resistors. I believe its midsize kit will have most of the above values in four to eight counts. Other values can be derived from values in the kit. For example, the prototype uses two 10K resistors in series in place of the 20K resistor.

JDR Microdevices also has a nice (more elaborate) resistor assortment that includes a parts bin. (Not a bad deal.)

The prototype used 1/4-watt resistors; 1/8-watt resistors may be substituted.

PART	VALUE	SOURCE	NOTES
(Capacitors)			
C1	10 µF	RS, JDR, Digi-Key	Tantalum preferred
C2, 6	1 µF	RS, JDR, Digi-Key	Tantalum preferred
C3	47 pF	RS, JDR, Digi-Key	Silver mica preferred
C4	.10 µF	RS, JDR, Digi-Key	
C5	22 pF	RS, JDR, Digi-Key	Silver mica preferred
C7	2.2 pF	RS, JDR, Digi-Key	Silver mica preferred
C8	10 pF	RS, JDR, Digi-Key	Silver mica preferred
(Hardware)			
M1		Radio Shack/JDR	Electret mic
L1	.2 µH coil	Make your own, JDR	10T 5/32-inch OD
L2	30–50 µH choke	Make your own, JDR	
ANT			Pseudo-resonant antenna is around 7 inches.

L1 can be made by wrapping 10 turns of enamel-coated wire around the ink cartridge of a cheap ballpoint pen (the cartridge serves only as a mold). The standard size ink cartridge will give you about a 5/32-inch OD coil (see Figure 5). The value is around .2 µH and can be adjusted by squeezing and spreading the coil. Once the coil is adjusted, you can freeze it in place with some wax or silicone rubber.

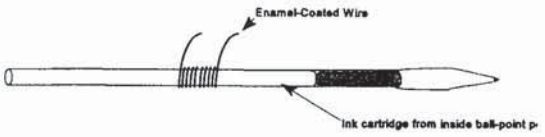


Figure 5. L2 can be made by wrapping about 20 turns of enamel-coated wire around a ferrite core. The prototype, however, used a 33 µH molded choke.

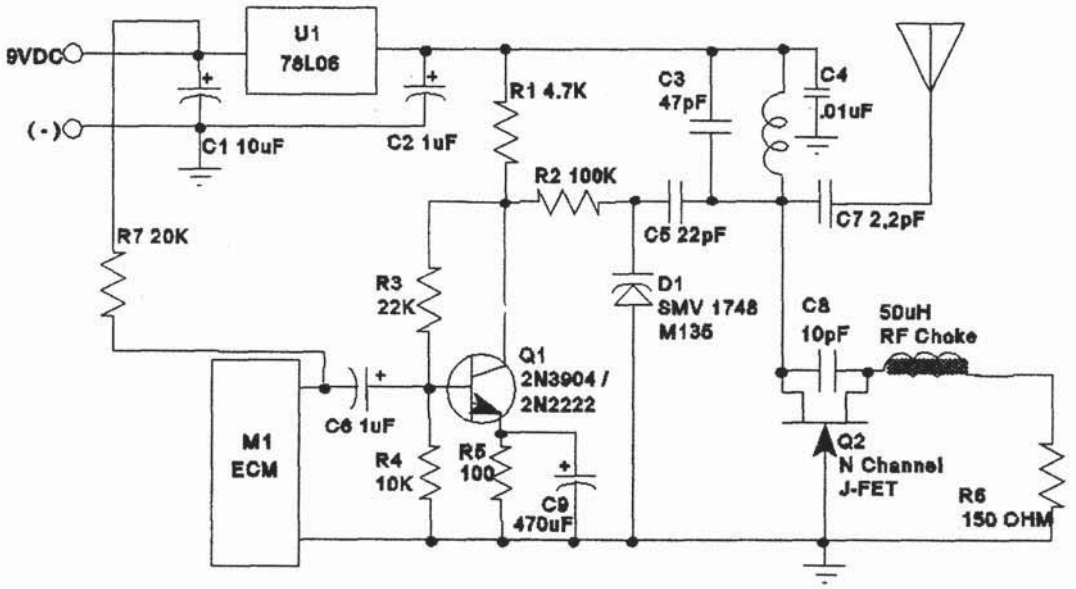


Figure 6. Schematic diagram for the SXC-49 FET-driven oscillator.

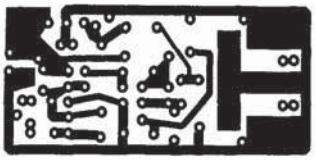
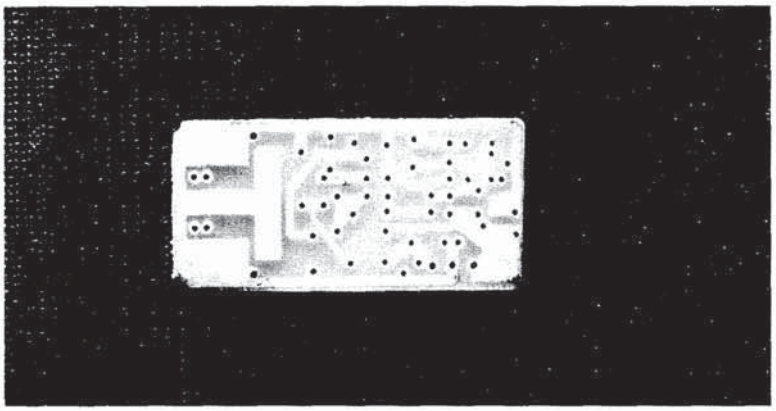


Figure 7. Foil pattern for the SXC-49.



SXC-48/49 combo PCB. Here is the SXC-49 PCB etched, tinned, and drilled. The image is about 10 percent larger than actual size. This PCB can be used for the SXC-49 room bug or the SXC-48 phone tap.

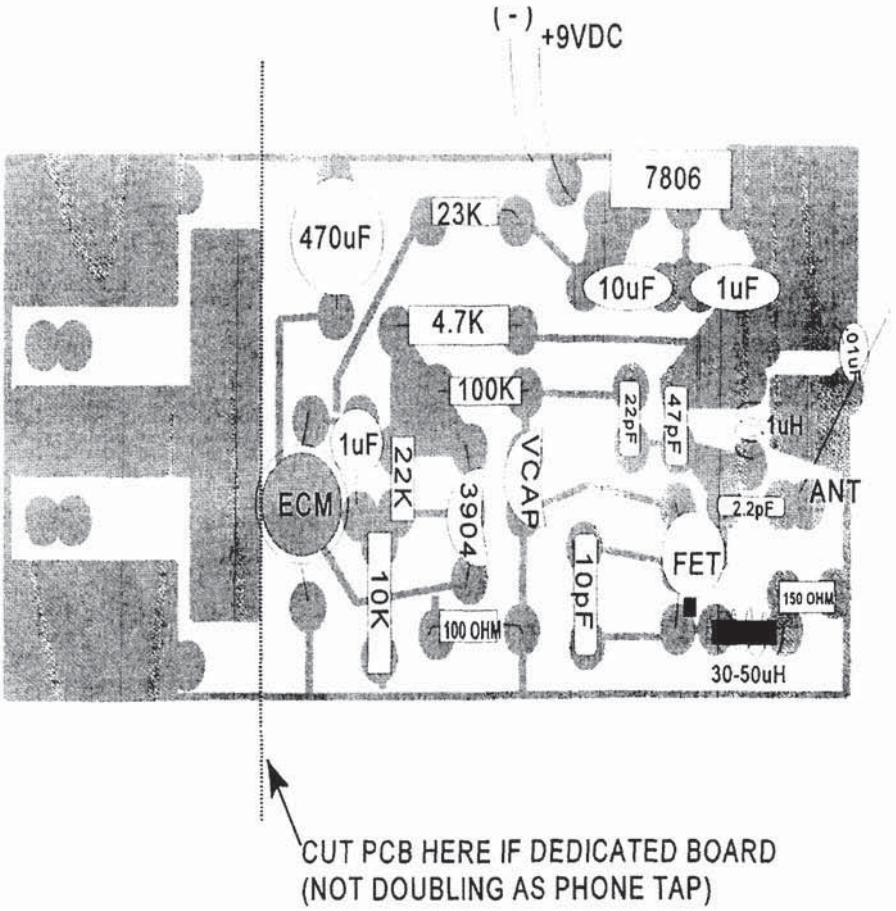


Figure 8. Stuffing diagram for the SXC-49.

Procedure

1. Follow the PCB and stuffing diagram for assembly.
2. Observe the polarity of electrolytic capacitors and voltage regulator.
3. Observe the proper placement of transistors and varactor.
4. Using a scanner, scan between 46 and 51 MHz to find the frequency.
5. Adjust the coil for 49 MHz operation by stretching and compressing.
6. Enjoy!

Theory of Operation

A steady +6 VDC is provided at the output of U1. C1 and C2 decouple the supply. M1, biased by R7, couples room audio through C6 to the base of Q1. R7 feeds directly from the battery for more efficient operation. The value of C6 (1 µF) is chosen for negligible reactance at audio frequencies. Q1, configured as a common emitter amplifier, offers low input impedance and moderate gain over a wide frequency range. The voltage divider composed of R1 and R3 reverse-bias the collector-base junction of Q1. R4 and R5 forward-bias the emitter-base junction completing a common temperature-stabilized bias arrangement. With the help of varactor diode D1, collector output of Q1 modulates the LC tank circuit composed of C3 and L1. Feedback for the tank circuit is supplied by Q2, the N-channel J-FET. Oscillator output is coupled through C7 to the antenna.

HOME-BREWED BUG
SXC-48 CRYSTAL-CONTROLLED FM PHONE TAP

This bug is a modified version of the SXC-49 room bug. For convenience in production and experimentation, the SXC-49 and the SXC-48 have the same PCB layout. The PCB for the SXC-49 room bug may be cut at the designated area on the layout, provided a jumper is used to complete the ground circuit, which would become open as a result.

Advantages of Crystal Control

The first and most obvious advantage of crystal control is dependable output frequency. If the bug is built right, you do not have to search for the proper frequency with your scanner. You should be able to turn your scanner on, set it for the bug's frequency, and listen in. Once tuned to the proper frequency, the operative will not have to make adjustments as the transmitter drifts. In fact, the operative could go out for pizza and confidently let a tape recorder take over for a while.

The next advantage is that of peak envelope power. The broadcast signal of a crystal-controlled transmitter is relatively more powerful than that of a transmitter left to drift. Technically, the output power is the same as far as the transmitter is concerned; it is different, however, for the receiver/scanner. With a drifting transmitter, the receiver is not tuned to the exact frequency of the transmitter most of the time. It is instead tuned to a less powerful off-peak signal. A receiver tuned to a crystal-controlled transmitter of the same frequency picks up the full peak signal 100 percent of the time.

Disadvantages of Crystal Control

One of the biggest problems with building a small crystal-controlled bug is dealing with modulation. There is somewhat of a catch 22 here: a crystal oscillator, which is designed to militantly keep its frequency, cannot be modulated as easily as an LC oscillator, which is very susceptible to modulation. This is because modulation is frequency change. If you use a crystal oscillator for rock-steady frequency, you will need a more powerful audio stage to modulate it. From our previous phone tap project, we already know that an audio-matching transformer in series with a phone line will act as a powerful audio stage. In fact, the prototype for that project used a 71.5K resistor in series with the transformer's output because the audio gain was so great.

Let's step back and look at this for a minute. The crystal oscillator's problem is that it needs a powerful audio stage. The audio transformer's problem is that its gain is too great. It seems that if we combine these two "problems" we have a solution for a crystal-controlled phone tap. I tried it. It works!

Parts List

In addition to the parts on the SXC-49 parts list, you will need the items listed here. Please note that some of the parts from the SXC-49 room bug are not needed in the SXC-48 phone tap:

- M1, the electret condenser microphone, is not needed because input will be taken from the phone line through T1.
- R7 is not needed because there is no microphone to bias.
- C9 is not needed because it is used to increase audio gain in the SXC-49; the transformer will be doing that in the SXC-48.
- C8 is ultimately not needed because it will be replaced by XTAL-1. You will, however, need to keep C8 in place during the "tune-up" phase, which will be explained later.

PART	VALUE	SOURCE	NOTES
T1	8-1,000-ohm audio	Radio Shack	Catalog item #273-1380
XTAL-1	48.000 MHz	Digi-Key	Part #X065-ND

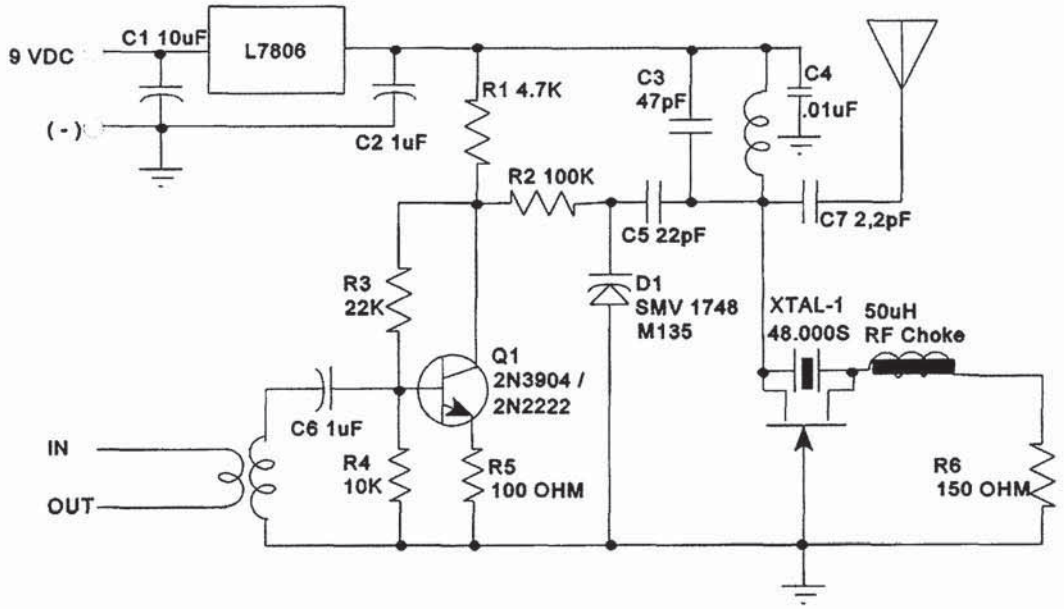


Figure 9. Schematic diagram for the SXC-48.

Figure 10. Foil pattern for the SXC-48.

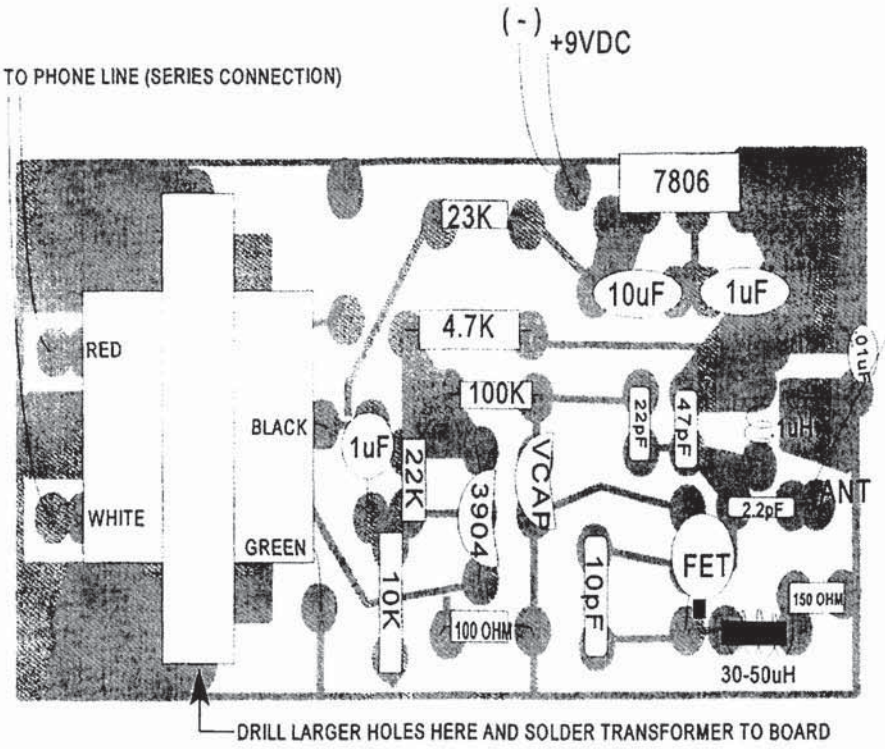


Figure 11. Stuffing diagram for the SXC-48.

Procedure

1. Follow the PCB and stuffing diagram for assembly.
2. For now, use a 10 pF capacitor in place of the crystal.
3. Observe the polarity of the electrolytic capacitors and the voltage regulator.
4. Observe the proper placement of the transistors and varactor.
5. Using a scanner, scan between 46 MHz and 51 MHz to find the frequency.
6. Adjust the coil for 48 MHz operation by stretching and compressing.
7. Follow tuning instructions below.

Tuning the Phone Tap

The 48 MHz series-resonant crystal in the feedback path of the oscillator is what keeps the bug on frequency. A simplified explanation for this is that the crystal provides a low impedance path for the feedback pulse at its resonant frequency. At frequencies other than resonance, impedance increases sharply. So, although it's true that the crystal will keep the transmitter on frequency, it's also true that the circuit must be tuned for 48 MHz (or damn near it) before the crystal can do its job.

The best way to do this is to first build the circuit with a 10 pF capacitor in place of the crystal. Then, tweak the coil (L1) by stretching and compressing it until the bug is oscillating at 48.000 MHz. The best way to check this is to put your scanner in "limit search" mode, scanning between, say, 47.900 MHz and 48.100 MHz until you get a reading. If this procedure is too aggravating for you, you may wish to invest in a multiturn coil or capacitor (of the appropriate value) in the tank circuit for fine-tuning. If you opt for this method, please be sure the component is of high quality.

Once you have the bug oscillating at 48.000 MHz, you may wish to freeze the coil in place with

some wax or rubber cement. By the way, this setup, even without the crystal, makes a damn good phone tap as long as you limit the input with a resistor or potentiometer as we did in our previous phone tap project.

Now, insert the crystal in place of the 10 pF capacitor. Set your scanner for 48.000 MHz. If the bug does not broadcast at 48 MHz, try tweaking the coil a bit. The overall capacitance of the tank circuit may have been affected by the capacitance of the crystal.

You must be aware that crystal oscillators are not usually this compact and typically call for more engineering (and components) for proper operation. Typical crystal oscillators do not overamplify the audio stage (as we are doing), but instead rely on one or more frequency multiplier stages to amplify its weak modulation. Because we are forgoing more elegant solutions in favor of a low component count, our circuit is somewhat tenuous. However, it is more than sufficient for its intended purpose.

Because of its inelegance, you will likely encounter some strange results while adjusting this circuit for optimal performance. For example, you may experience strong modulation on spurious sidebands, say 48.190 MHz and 47.810, with weak modulation of the carrier frequency (48 MHz). Keep in mind that these aberrations result from improper tuning. Also keep in mind that ideal results will never be achieved with this bare-bones circuit. When you have a decent signal at 48 MHz with decent modulation, you have succeeded.

Theory of Operation

Operation of this inelegant yet effective crystal-controlled FM phone tap is essentially the same as the SXC-49, with the following exceptions:

- Input is taken from T1, which is connected in series with a standard telephone line.
- Through C6, the transformer output is coupled to Q1, which is purposely driven to near overdrive to compromise for an expected difficult modulation of the tank circuit (due to its crystal control).
- The N-channel J-FET supplies a feedback pulse for the tank circuit. The 48 MHz crystal, operating at series resonance, is placed in the FET's feedback loop to lock oscillation at 48 MHz.

ALTERNATIVE USES

An FM phone tap can be used with a tape recorder and be converted to a sales and marketing aid for your business. By reviewing calls, you can improve your sales technique. The wireless operation will save you from the hassle, expense, and general ignominy of having to drill holes in your walls to run wires.

By reviewing your conversations with customers, you can refine your sales pitch and increase profits. For this use, you will need to check the applicable state laws. In many states, such marketing aids are illegal unless you disclose to your prospects, in advance, that the call is being recorded. If they object, you must shut off the tape recorder or terminate the telephone call.

I see nothing wrong with converting an FM room bug to a mini radio station for yourself or a child or grandchild, provided that it is used in accordance with FCC regulations. Similarly, this device may be converted to a baby monitor to listen in on a sleeping child.

The best alternate use I have found for my SXC-49 room bug is not in a room at all, but outside. One of my favorite extracurricular activities is sky watching. I like to check out the planets and certain "Messier objects" with a reflecting telescope made by Meade Instruments Corporation and carrying a price tag that'll fog your goggles. I set my telescope up out behind my house, sometimes carrying it far up a hill to get away from the ambient light, which always interferes with good viewing.

Well, on a cold winter night in New York, you can view the sky for about 15 minutes before your toes begin to curl and turn black from frostbite. Frequent trips back inside the house are thus required. Can you see the problem with this? I have to go back to my house while my telescope remains outside perched atop a hill. Any junkie from the city who happens to spot it there no longer has to worry about where his next several heroin fixes are coming from. What's a junkie doing on top of a suburban hill on a cold winter night? Looking to steal something, that's what. Solution?

I have an SXC-49 room bug built into the base of the equatorial mount of my telescope. The antenna hides inside one of the tripod legs. I keep a scanner in my house tuned for 47.600 MHz (I threw an extra turn on the coil, so technically it's not an SXC-49, but "SXC-47.6" doesn't sound as good). When I'm in my house warming up, I keep an ear on the scanner. If anybody comes near the scope, I know about it. In fact, I'm listing to my telescope as I type this. My telescope is outside tracking M31, the Andromeda Spiral Galaxy. One time, while vacationing in "Cat's Kill," this setup saved my telescope from a finger-happy tourist, who now has one less happy finger.

Notes on Use

Above, I told you that when using my SXC-49 as a telescope sitter, I keep my scanner set for 47.6 MHz. Let me just clarify this. The room bug is turned on inside the house, where it's warm. I then scan between 45 and 47 MHz until I find the correct frequency. Sometimes, you think you have found the correct frequency, but after walking 20 feet or so you lose it, so you had not found the correct frequency after all. You found a harmonic or image of the fundamental frequency. While staying put (20 feet away from the bug), add or subtract 900 KHz from the frequency you are scanning; 900 KHz is a very common image frequency, though there are others. For instance, if your weak signal is at 47.000 MHz, see what happens at 47.900 MHz. If that doesn't work, try 46.100 MHz. If neither of these alternative frequencies work, set your scanner to limit-search 3 MHz below to 3 MHz above the weak signal. In our example that would be 44 MHz to 50 MHz. See if you can find a better signal. If you do, use the 900 KHz trick again to make sure you've got the fundamental frequency. With this design, the correct frequency should have a 900 KHz image on both sides of it when the scanner is very close to the bug. This verification technique does not always work, though. If you have a strong signal that does not drop off too fast as you walk away, then you probably have the fundamental frequency. But . . .

If you take the bug outside where it's 1°F, the bug will begin to adjust itself slightly. Be prepared for this. My telescope monitor bug begins to climb slowly but steadily in frequency once outside in the cold. From experience, I have learned to set my scanner to limit search between 47.550 and 47.750 (150 KHz on either side of the fundamental). If you use this method, turn the squelch up so the scanner will scan as the bug drifts off frequency. For the first few minutes you will hear the signal fade away, at which time the scanner cracks up with some brief white noise and then adjusts itself to the next frequency. After three minutes or so, when the temperature of the bug stabilizes, this will happen less and less frequently. After 15 minutes the bug will give you a dependable signal again.

SUMMARY

The projects in this chapter demonstrate the most important fundamentals of design, construction, and operation of FM transmitters. When you feel as though you have a thorough understanding of the principles involved, you may wish to make your own refinements and customizations to these circuits. Again, remember to check all applicable laws before using these devices in any manner. Be sure you comply with FCC regulations pertaining to unlicensed broadcasts.

CHAPTER 3

BUILDING A DTMF DECODER

WHAT IS A DTMF DECODER?

A DTMF decoder is a device that decodes Touch-Tone™ telephone beeps. When hooked up to a telephone line, tape recorder, or scanner, the ideal decoder will graphically display the DTMF tones on a screen.

The operative using this device can see what tones his subject sent out over the wires and gain such information as phone numbers of the subject's consorts and business associates. A subject's bank account number, PIN code, credit

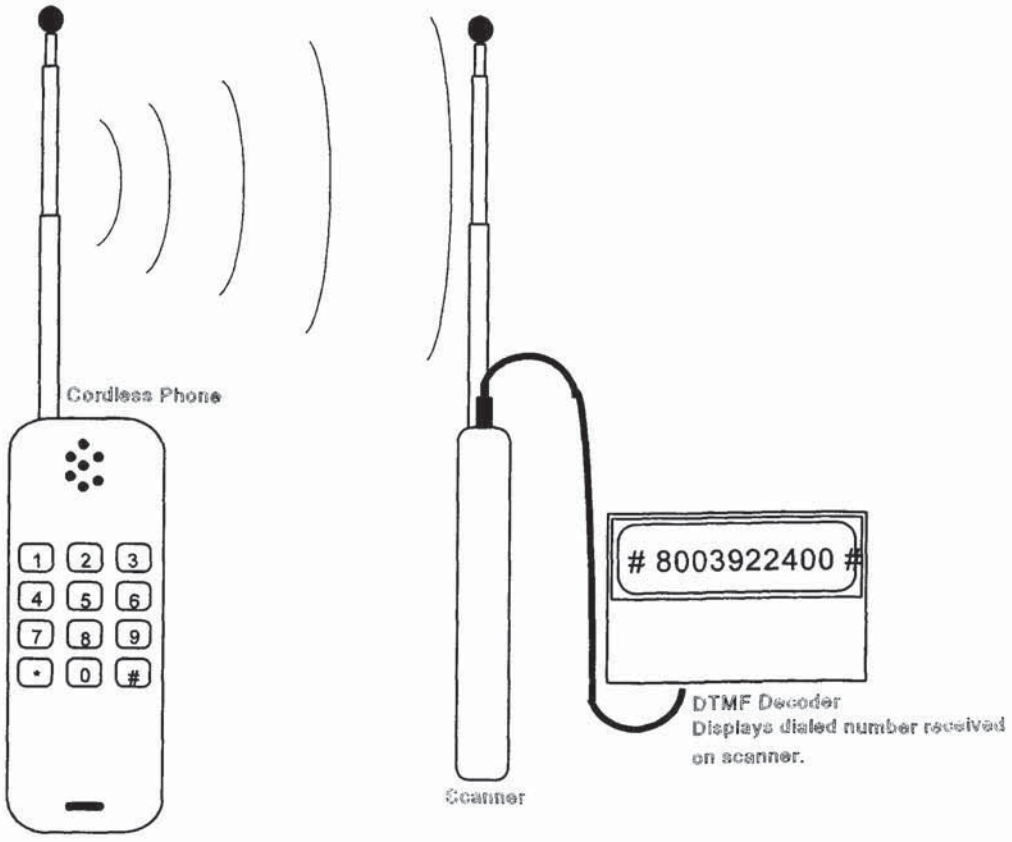


Figure 12. The fast track to gathering key information on your subjects!

card number, and voice mail password can also be gleaned from using this wonderful device. Generally, any numbers the subject punches into his phone for any reason can be decoded. The DTMF decoder we will be building is also capable of decoding special TelCo signaling characters A, B, C, and D, also used by ham radio operators. More on these later.

"A marvelous product! " you say. "Just think of all the wonderful things I could do with this device! I'll save hundreds of investigative hours! Let me run out to the store and buy one today!"

I'll save you a day's "wild decoder chase" and tell you the bad news up front. This gadget is not available in stores. That is to say, when I first heard of its unavailability, I thought it was bad news. Now that I'm the only detective on the block who owns a DTMF decoder or even knows what one is, its lack of availability appeals to me. Certainly, there are advantages here!

What Is DTMF?

DTMF is an abbreviation for dual-tone multiplexed frequency. In the late 1960s, TelCo engineers began to face the reality that pulse signaling was too slow to meet the growing demand of existing telephone lines and equipment. In addition to its slowness in signaling, pulse signaling suffers pronounced distortion over great distances and requires a DC path in the communication line. Either billions of dollars would need to be invested in more lines, transformers, and switching stations, or a better system would need to be invented. That system was DTMF signaling.

With DTMF, a "0" or "9" could be sent down the line just as fast as a "1" or a "2." This was not the case with pulse dialing. Remember those phone numbers that took a long time to dial? Like (555) 999-9000 when you had to wait for the dial to return from its long trip to the big 0 with the foreboding OPERATOR in curved print beneath it? Comparatively speaking, 555-1212 was much more fun to dial, especially the 1212 part. Remember?

Well, I hate to disappoint you, but the fun and easy push buttons that came along later were not for your convenience. The speed and utility of that technological advance benefited the TelCo.

Combined with technological advances of the 1970s, DTMF became faster and more useful than ever thought possible. An entire telephone number could be sent over the wire in well under a second. Granted, millions of dollars were spent implementing this new technology, but billions of future dollars were saved. Big corporations like this kind of math.

What Exactly Is a DTMF Tone?

As suggested by its name, a DTMF tone is the product of two frequencies. The tones were chosen so as not to be harmonically related, thereby minimizing the chance of false signaling due to human voice and other stray signals. Another criterion was to eliminate the risk of nonsignaling because of phase cancellation resulting from intermodulation of

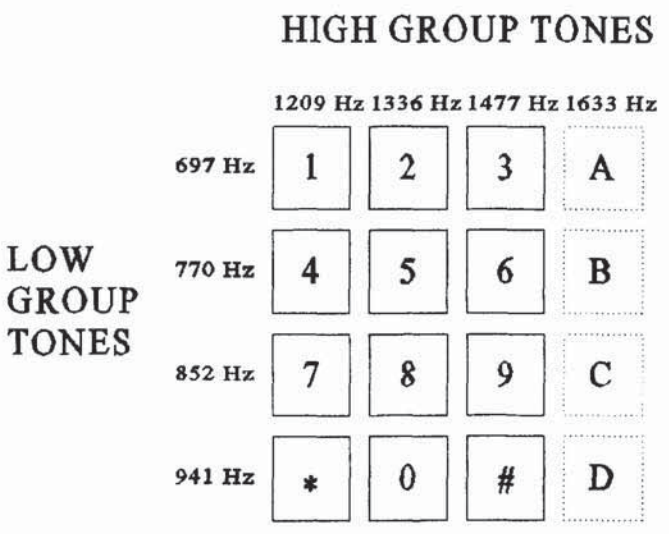


Figure 13. As its name suggests, a DTMF tone is composed of two tones. One tone is taken from the high group, and the second tone is taken from the low group. Use this chart if you ever desire to know which two frequencies make up a particular DTMF tone. For example, the digit 5 is composed of 1,336 Hz and 770 Hz.

the two tones—two obviously important considerations for TelCo engineers.

The matrix in Figure 13 depicts the final choices of the engineers. You will see that each tone is the result of one tone from a high-frequency group and one tone from a low-frequency group. The four frequencies in each group form a matrix that yields 16 possible DTMF tones.

The DTMF decoder design I opted to publish is a modular design. The individual modules are these:

- Decoder module
- Binary readout module
- Seven-segment readout module
- LCD readout module

THE DECODER MODULE

The decoder module is the heart of the DTMF decoder. It contains the Mitel™ 8870 DTMF decoder chip and supporting hardware. Since this board is going to be the heart of each DTMF decoder project in this book—be it the LCD, light-emitting diode (LED), or binary readout version—it contains the protective input circuitry and power supply circuitry. Note the eight-pin connector; this is how the decoder module will mate with all other modules.

Parts List

PART	VALUE	SOURCE	NOTES
(Semiconductors)			
IC1	Mitel 8870	CTS, author	DTMF decoder chip
IC2	+5 VDC regulator	Radio Shack	7805 or LM340T5
D1, 2 , 3	15 V 250 mW	Digi-Key 1N5245BCT	Zener diodes
D4	1N4001	Widely available	
(Resistors)			
R1, R2	110 KΩ, 1W, 1%		
R3, R4	110 KΩ, 1/4W, 1%		
R5	52 KΩ, 1/4W, 1%		
R6	220 KΩ, 1/4W, 1%	Widely available	Mitel's suggested value
R7	68 KΩ, 1/4W, 1%	Widely available	Mitel's suggested value
R8	368 KΩ, 1/4W, 1%	Widely available	Mitel's suggested value
R9	2.2 M KΩ, 1/4W, 1%		
(Capacitors)			
C1, C2	.01 µF 630 V	Digi-Key EG103	630 V for ring voltage
C3	.1 µF	Widely available	
XTAL1	3.579545 MHz	Widely available	
(Hardware)			
S1	SPST	Digi-Key EG1901 (optional)	Power switch
9 V battery clip		Widely available	

The component values listed are those suggested by Mitel Corporation per its application note MSAN-108. During my research and previous prototypes, I've substituted resistors with the closest common values at 5 percent tolerance without any noticeable problems. Prototypes substituted 200 V caps for C1 and C2 with no problems. For continuous phone-line hookup, stick with 1 W resistors for R1 and R2.

The plug and jack are highly recommended, and the PCB is laid out for the Digi-Key part numbers given (drill 5/64-inch holes). For testing, though, you may use alligator leads.

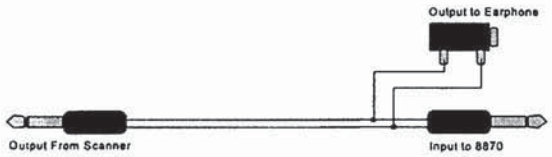


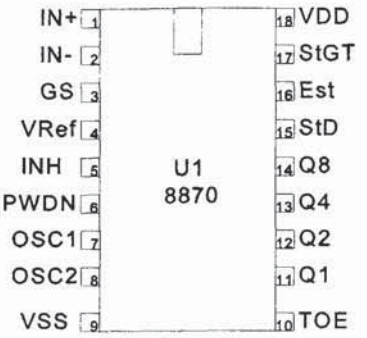
Figure 14. A homemade "Y" adapter will allow you to listen to DTMF tones while you decode them.

Decoder module prototype with LCD readout (built on a single board) hooked up to a scanner and Radio Shack tape recorder. Output from the scanner is taken from the headphone jack through a homemade "Y" adapter. Output from the "Y" adapter is fed into the decoder module input jack and the AUX INPUT jack of a tape recorder. Earphone output is taken from the recorder. To do this, the recorder must be placed in record mode. Keep the tape paused until something exciting happens!

8870 Decoder Chip

The 8870 decoder chip is a marvelous piece of engineering and is worth looking at. For this reason and for use as a quick reference, a pinout is shown along with the schematic.

Pinout for Mitel's 8870 DTMF Decoder Chip



IN +	Non-inverting Op-Amp input	VDD	+5VDC
IN-	Inverting Op-Amp input	StGT	Steering / Guard Time Circuit
GS	Gain Select	ESt	Early Steering Output
VRef	VDD/2 biases at mid-rail	StD	Delayed Steering (Data Valid)
INH	Inhibits A, B, C, D tones*	Q8	Binary 8's placeholder
PWDN	For "sleep" mode*	Q4	Binary 4's placeholder
OSC1	Clock Input 3.579545Mhz	Q2	Binary 2's placeholder
OSC2	Clock Output	Q1	Binary 1's placeholder
VSS	Ground (0VDC)	TOE	3-State Output Enable

*These pins are tied low internally. They are active high and we do not use them.

Figure 15. Since it's such a "kewl" chip, I thought I'd include its pinout. Studying this pinout will help you better understand how the chip functions.

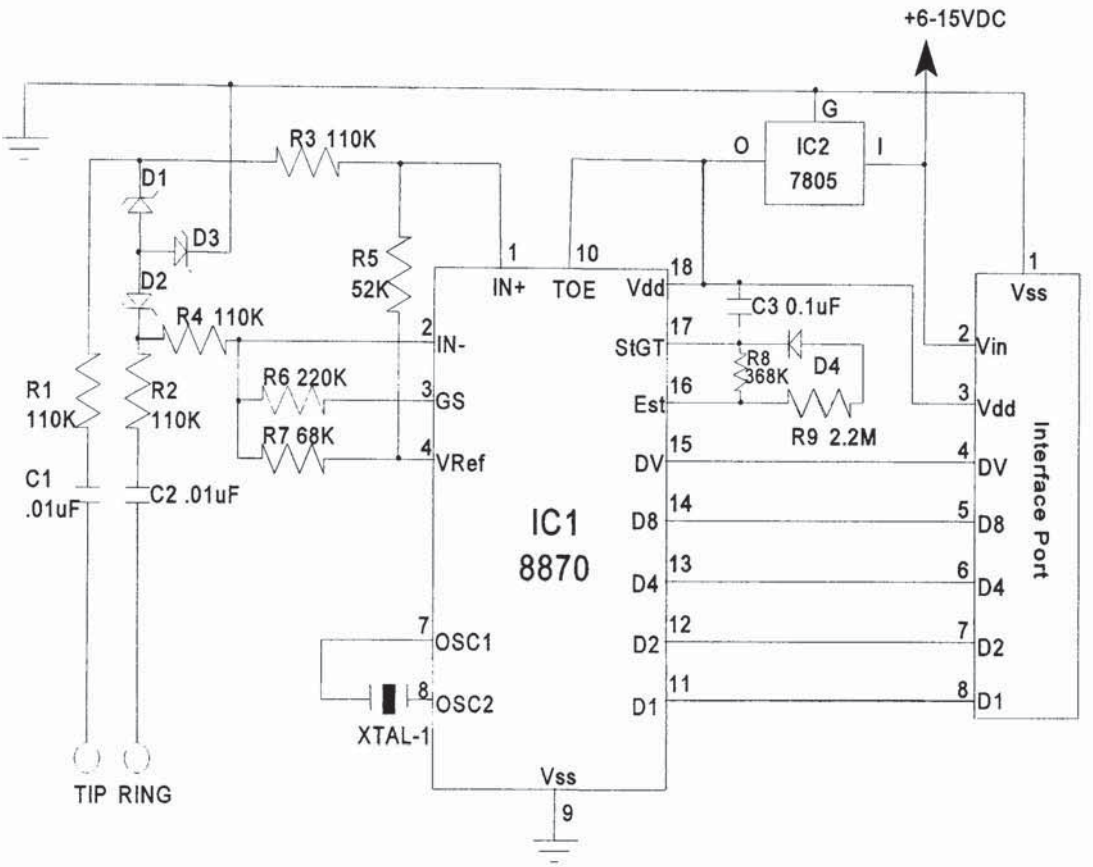


Figure 16. Schematic for decoder module.

Theory of Operation

(Please refer to Figure 16.) DTMF tones are received at the balanced line input labeled "TIP" and "RING." This input configuration is virtually identical to that suggested by Mitel Corporation in its Applications reference. The configuration allows the decoder to be connected directly to a telephone line, if desired. Input can also be taken from the "Tape Out" jack of a scanner or the "AUX" output of a tape recorder. Actually, this configuration can handle just about any practical line-level input. I've even wired the input in parallel with a scanner speaker (not recommended) with remarkable success.

Adjustment of R6 at pin 3 will probably allow for microphone level input, but I have not tested this because I see no practical use for a microphone input. Virtually all electronic devices manufactured today have auxiliary outputs as standard equipment, and a live telephone may be substituted for a microphone if a situation ever calls for microphone input.

C1 and C2 isolate DC line voltages (such as from a telephone line or speaker) from the decoder chip while allowing AC to pass. The zener diode configuration protects the decoder chip from the 90 VAC telephone ring signal. Never connect the decoder chip to a telephone line without this protective circuit!

The inputs of the op-amp are biased at 1/2 V_{DD} by the reference voltage available at pin 4, setting the op-amp for unity gain. Although the decoder chip is comfortable with a wide input voltage range, volume adjustments, when available, may help optimize performance.

The RC time circuit at pins 17 and 18 sets the length of time a DTMF signal must be present before the decoder "believes" it is actually "hearing" one. This is known as the tone present guard time (GTp). The idea is to set GTp long enough so that false "hits," such as those caused by human voice, are eliminated.

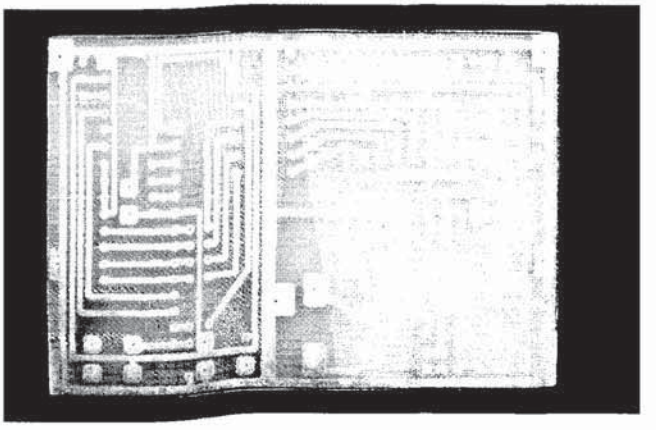
This circuit also works in reverse setting the tone absent guard time (GTa). A long GTa ensures that a valid DTMF tone will register even if it is interrupted by short bursts of noise.

Our decoder, however, is a surveillance device designed to detect tones before any conversation is present. We must also keep in mind that DTMF output from a scanner or tape recorder will be accompanied by a lot of electronic noise. Thus, I have used Mitel's suggested design for a short GTp and a long GTa. In reality, R9 and D4 may be omitted entirely without significantly compromising performance.

When a DTMF signal is detected, a binary representation of the DTMF tone is latched at pins 11 through 14. After a short delay, allowing the output latch to settle, pin 15 goes high, indicating that a valid DTMF signal has been received and is ready to be read.

We refer to pin 15 as the "data valid" (DV) line, and this signal is used to tell the readout module when to read the output latch. The only module that really relies on the DV line is the LCD readout module because it is microprocessor controlled. The DV signal can also be used with a ripple counter and memory chip to make a memory buffer for your decoder.

Reading through the foregoing time sequence, one might come to believe that a tremendous amount of time goes by while the chip is doing its job. In actuality, these transactions transpire in microseconds.



Decoder and LCD module PCBs. The layouts were designed so that the builder has the option of integrating them onto one PCB (as shown). The PCB was made using the positive photo-resist method as outlined in Chapter 1. Large square pads in the upper corners of the PCB and two-thirds of the way down each side serve to accommodate the LCD readout.

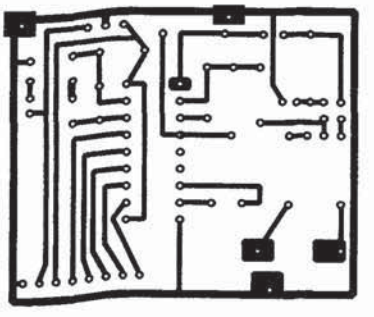


Figure 17. Foil pattern for decoder module.

An 11-digit phone number can be decoded and placed on an LCD screen in about a second.

Test Points

After hooking power up to the decoder module, the first thing you should test for is a regulated +5 VDC between ground and the P+ side of the regulator chip. This regulated +5 VDC should also be present at pins 10 and 18 of the 8870 chip. The middle pin of the voltage regulator and pin 9 of the 8870 should be at 0 VDC. If any of these test points do not check out, disconnect the power immediately and check your work.

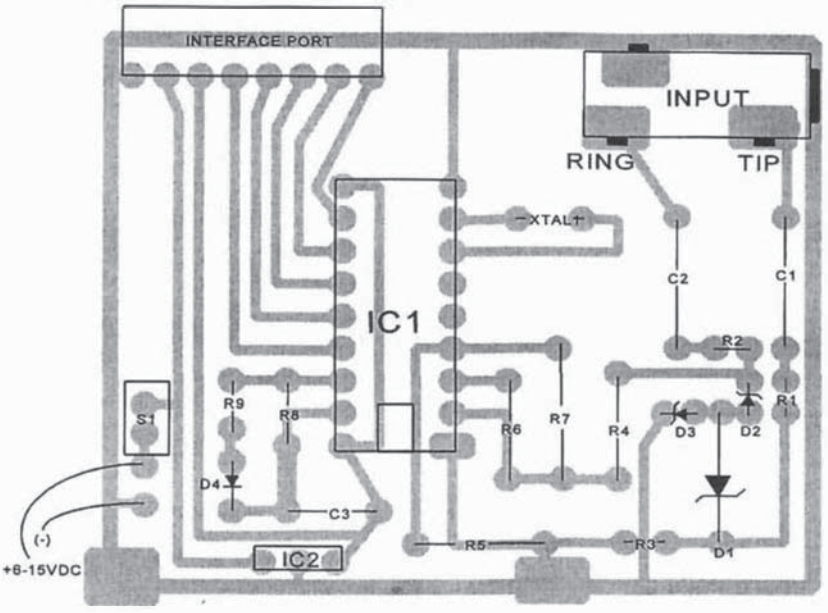


Figure 18. Stuffing diagram for decoder module.

Correct functioning of the 8870 chip can be tested by hooking the balanced line input (alligator clips or jack assembly) in parallel with a live phone line. Pick up any extension on that line, dial "1," and then hang up. If your decoder is working properly a binary "1" (0001) should be present at pins 11 through 14 of the 8870 chip. Use a multimeter to read the DC voltages at these pins. Pin 11, the LSB, should read +5 VDC, and pins 12 through 14 should read 0 VDC to represent a binary "1." Check these voltages for digits 0 through 9 as well as the * and # keys. The readings should follow this chart in Figure 19.

If pins 11 through 14 do not change at all as you press keys on the telephone, make sure the telephone you are using is

- either "up-line" or at the same junction as the decoder or
- set for "tone dial" and NOT "pulse dial."

Once you're confident that the telephone setup is OK, check your work at the input circuit of the 8870 chip. Make sure of the following:

- Orientation of zener diodes is correct.

D	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
0	1010
*	1011
#	1100
A	1101
B	1110
C	1111

Figure 19. Use this chart to determine what DTMF tone corresponds to the binary reading at the 8870's output latch.

- Values of C1, C2, and all resistors are correct.
- Tip or ring paths are not shorted to ground (such as by hardware, screws, standoffs, or other "project box" fixtures).

If problems persist, make sure that pin 1 of the 8870 is in the square hole, look for opens and shorts in the PCB traces, look for cold solder connections (broken wires if breadboarding), etc. Keep in mind that this design was tested extensively over the past two years and that improper function is most definitely due to improper assembly!

You will not be able to test for A, B, C, or D, but if all other values check out, you can bet the 8870 chip is properly configured and doing its job. Usually, if one digit does not register properly, some or all of the others will follow suit. If you are getting bad readings, disconnect the power and check for opens and shorts at pins 11 through 15.

THE READOUT MODULES

BINARY READOUT MODULE

A simple binary readout module can be constructed to read the output of the decoder module. The binary readout module is a nice educational demonstration and makes a good test circuit for the decoder module. If you have trouble envisioning the binary counting scheme, building this circuit will help.

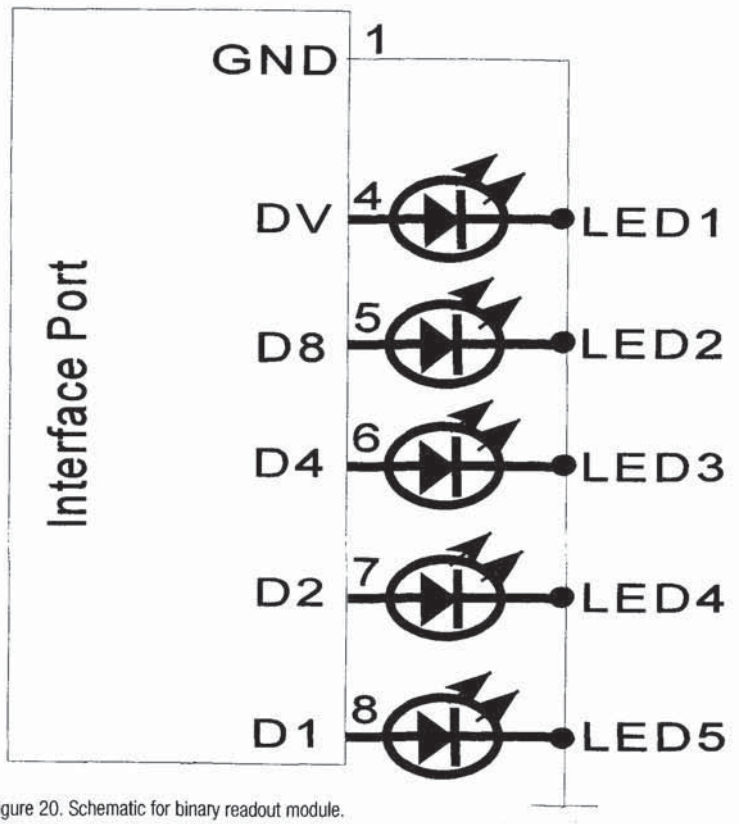


Figure 20. Schematic for binary readout module.

Theory of Operation

All that's going on here is that we're placing an LED between one bit of the output latch and ground. If that pin goes high, the +5 VDC will travel through the LED to ground, causing it to light up. This is a nice visual test for the 8870 output latch and decoder module interface. In a pinch, this setup can be used to decode recorded DTMF tones.

D1 indicates when a valid tone is present at the output latch of the 8870. While testing, hold down any key on the telephone keypad and this LED will stay lit. Release the key and the LED goes out, indicating the DV has gone low and a valid DTMF tone has been received. D2 is the most significant bit (MSB), and D5 is the least significant bit (LSB).

A quick PCB would look like Figure 21 on next page.

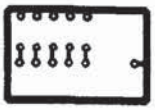


Figure 21. Foil pattern for binary readout module.

This PCB assumes that you have chosen the right voltage LEDs so that resistors are not needed. It would be stuffed like this:

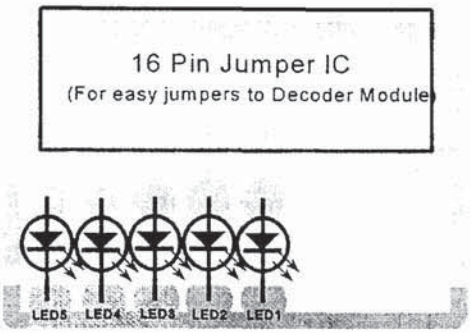


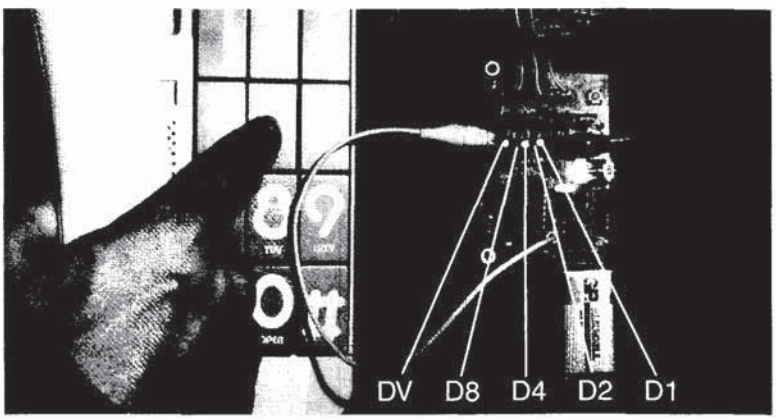
Figure 22. Stuffing diagram for binary readout module.

But a quick-and-dirty version can be built right on top of a 16-pin DIP IC socket, which is what I opted to do.

Parts List

PART	VALUE	SOURCE	NOTES
LED 1-5	5 VDC	Radio Shack	Or use resistors with 3-volt LEDs
Jumper IC	16 pin		For easy jumpers to decoder module
DIP socket	16 pin	Radio Shack	To fit jumper IC for decoder module interface

Here is a quick mock-up in action:



Quick-and-dirty binary readout for functional demonstration. This unit was built with LEDs on a 16-pin DIP socket. Alligator test leads were used to tie the LED cathodes to ground. While the "5" key is depressed, the DV line remains high, and therefore the LED remains lit. D1 and D4 LEDs are also lit, representing a binary "5" (0101). When the "5" key is released, the DV LED will go out, but the binary "5" will continue to be displayed until the next tone is received.

SEVEN-SEGMENT READOUT MODULE

A seven-segment readout module may be sufficient if all your decoding jobs are recorded on tape or if you build a memory buffer for your decoder.

Parts List

PART	VALUE	SOURCE	NOTES
LED1	7-seg. CC	Radio Shack	Catalog item #276-075
IC1	4511	Digi-Key	BCD-to-7-segment decoder Part #CD4511BCN-ND
R1-7	1/4 W 100 Ω		
IC socket	14-pin DIP	Widely available	(Optional) for 7-seg.
IC socket	16-pin DIP	Widely available	(Optional) for 4511
IC socket	16-pin DIP	Widely available	(Optional) for jumper IC
Jumper IC	16-pin DIP		(Optional) for EZ jumpers to decoder module

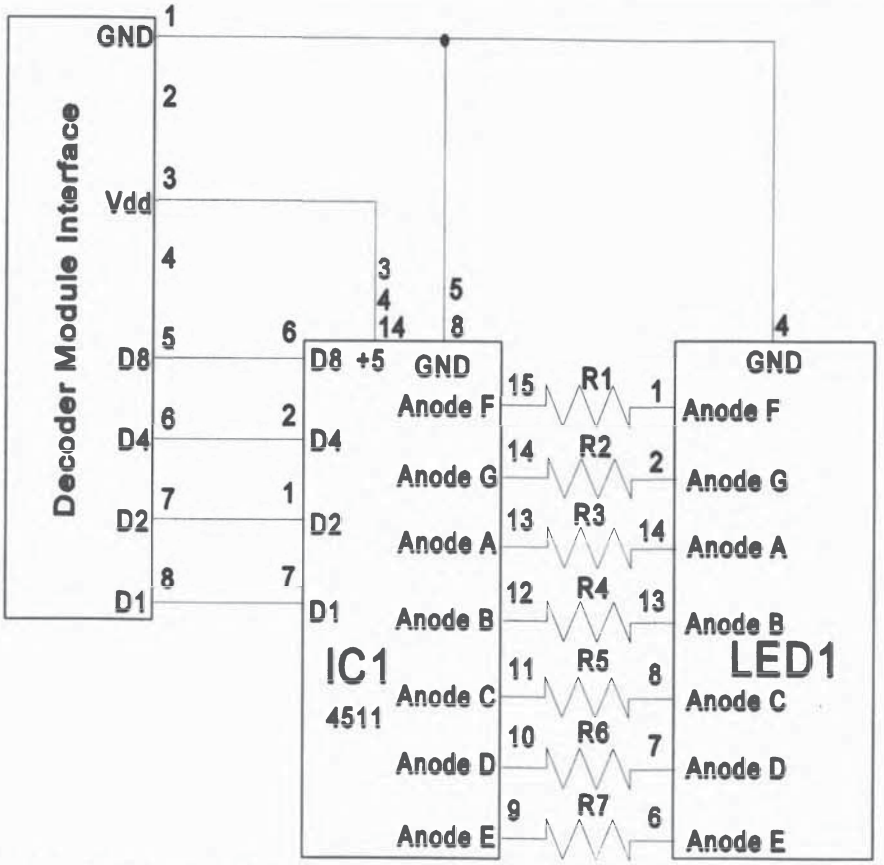


Figure 23. Schematic for seven-segment readout module.

Theory of Operation

Pin 1 of the interface port completes the ground circuit to the decoder module. Binary coded decimal (BCD) is received at IC1 via pins 5 through 8 of the interface port. IC1 decodes the BCD, and pins 9 through 15 drive LED1, the seven-segment display, to ultimately give a decimal representation of any DTMF tone decoded by the decoder module.

It's interesting to note that the seven-segment display module can be used as a test circuit or readout module for other devices with four-bit binary output (watch your voltages!).

The prototype used 100-ohm resistors between the outputs of IC1 and the individual LED segments. You may wish to experiment with other values to make your readout brighter or dimmer.

As an experiment try connecting pin 4 of the interface port (DV) to pin 9 of the seven-segment display using a 100-ohm resistor. The decimal point will light up while the DV line is high (for as long as you hold down the telephone key).

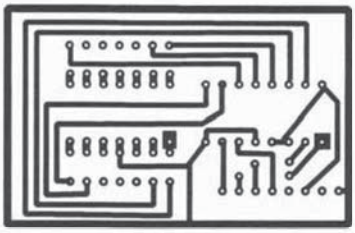
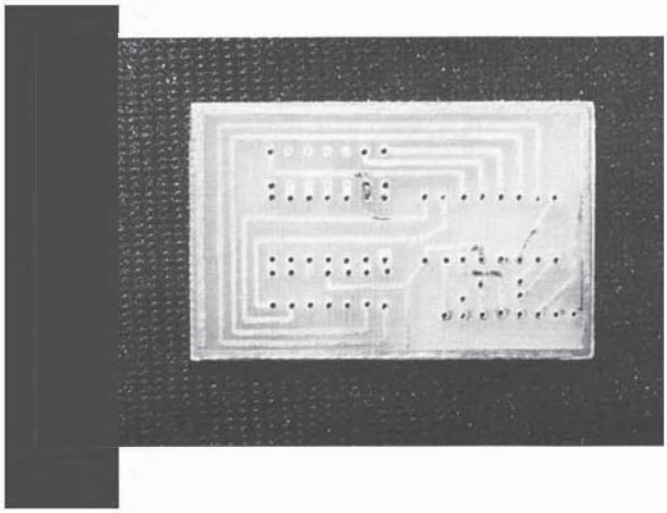


Figure 24. Foil pattern for seven-segment readout module.



This is the same PCB used for the prototype shown in the photo on page 45. When drilling, try to remember that unused solder pads need not be drilled. I remembered about halfway through the drill job on this one. When working intently, it's easy to get carried away. Don't make extra work for yourself!

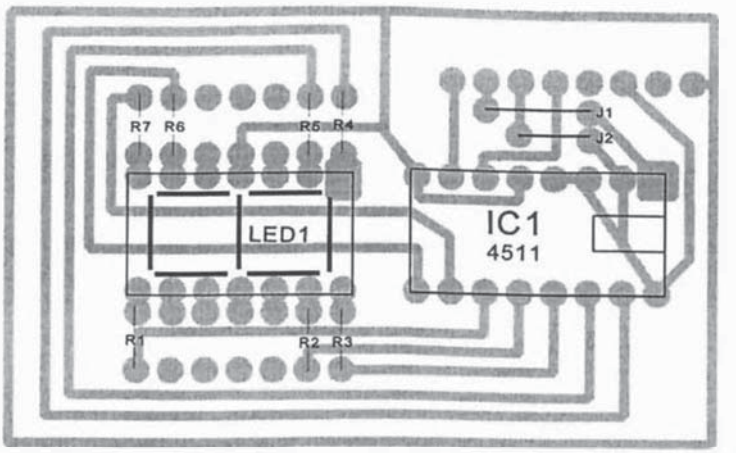
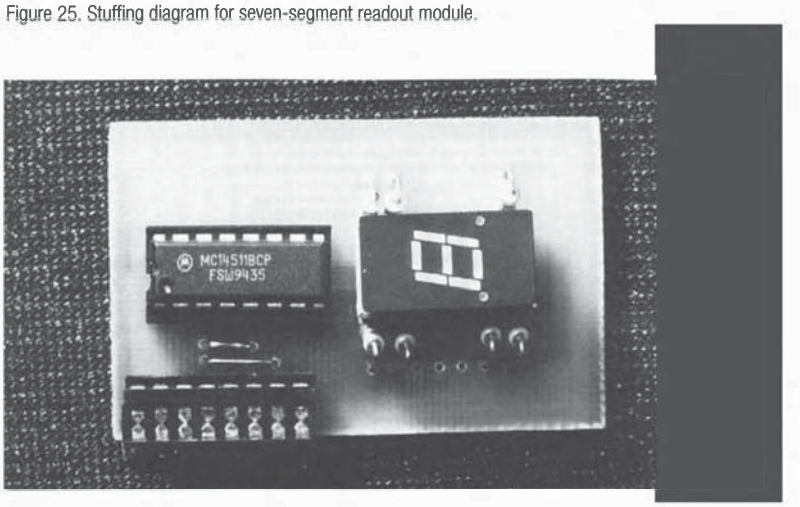


Figure 25. Stuffing diagram for seven-segment readout module.



This is a photo of the completed seven-segment readout module with a jumper IC in place for easy jumpers to the decoder module. Clipped component leads were used for J1 and J2.

Procedure

1. Remember that any substitution of the seven-segment display must be pin for pin.
2. Refer to schematic, PCB, and stuffing diagrams during assembly.
3. Use clipped component leads for jumpers.

Testing

Connect the LCD readout module to the decoder module using jumpers, or a 16-pin jumper IC. Connect the decoder module to the phone line. Turn on S1 of the decoder module and verify these voltages on the readout module: pins 3, 4, and 14 of IC1 should read 5 VDC. Pins 5 and 8 of IC1 and pin 4 of LED1 should read 0 VDC. If these values do not correspond, recheck your work.

Dial some numbers, hanging up regularly to prevent unwanted connections (especially long-distance ones!).

If numbers display improperly, check for proper interface with the decoder module. Check pins 7, 1, 2, and 6 of BCD-to-seven-segment decoder; they should correspond to the 8870's output latch (pins 10 through 13). The circuit is not complicated.

Notes on Use

Because it has no built-in memory, this display module is best for decoding DTMF tones from the output of a tape recorder. It can be used with a scanner if you're really on top of things. If the same number is dialed two or more times in a row, the display will not change. Therefore, you must be listening to the tones to determine this. For example, if you hear two tones that sound the same and the display does not change, you can safely assume the same number was dialed twice.

The "0," "*," and "#" keys will display as a blank screen. You will not see a "0" on the seven-segment display because a "0" is actually represented as a "10" (1010 in binary) at the 8870 output latch. The BCD-to-seven-segment decoder can only decode digits 0 through 9. Any number greater than 9 (1001 in binary) will display as a blank. By using common sense, however, you should be able to distinguish a "0" from a "*" or a "#" keypress. For example, "*" and "#" will not be part of a telephone number so a blank screen would represent a "0" in this case. A blank screen at the end of a password or account number is probably a "#" keypress, which is typically used as an "ENTER" key. A blank screen before a number is dialed is probably a "*" keypress used to activate or deactivate some TelCo feature, such as call waiting (*70 to suppress), call forwarding (*72 on, *73 off), caller ID (*67 to suppress), ring back (*69), etc.

LCD READOUT MODULE

Ever wanted a DTMF decoder with an LCD readout and on-board memory? So did I. Companies pop up from time to time advertising such units, but they are usually quite expensive. One company advertised one for $325. Ouch! According to the ad, it had little more functionality than the one we're about to build.

I've always been afraid to order from these fly-by-night companies. What if their design used some obscure part that fails after they go out of business? What if the firmware crashes right after the company does? We've all heard the horror stories.

Those were the concerns I had four years ago as a consumer in the market for a DTMF decoder. After a good deal of research, I decided my best bet was to build my own. Once finished, I had a DTMF decoder with LCD readout and on-board memory that I knew exactly how to maintain. Even more rewarding was what I had learned in the process.

In this section, we will construct the LCD readout module. Once interfaced with the decoder module, you will have a complete DTMF decoder with LCD readout and on-board memory. It is the same one I designed four years ago when I was a disgruntled consumer—except that you'll have the benefit of all my experience and several refinements.

The most expensive part of the LCD readout module is the BS1-IC, or BASIC Stamp™, which is a product of Parallax Corporation. These little buggers are still selling for $35 per unit, but I am expecting the price to drop as more and more hobbyists bypass the BS1 in favor of programming their own PIC microcontrollers at an 80 to 90 percent savings.

The BS1 is so popular and multifunctional, however, it makes sense to use it as the "brain" of our LCD readout. If you're an avid electronics hobbyist, you may already own a BS1. If so, you'll have no reason to buy another unless you insist on having dedicated boards for every project you build. If you don't yet own a BS1, you will need to purchase one to build this project. The expense is justified because this chip is easy to work with and can be used in many other projects. Another important justification is that the BASIC Stamp™, in my opinion, is the best way for a beginner to be introduced to the fascinating world of embedded controllers.

I recommend buying the whole BS1 programming package available from JDR Microdevices, Digi-Key, or Active Electronics. The package includes the BS1-IC, the BS1 Carrier Board with prototyping area, a PC interface cable, programming software, and user manual that contains many

projects and application notes. You will need the software unless you have a friend who will program the Stamp for you.

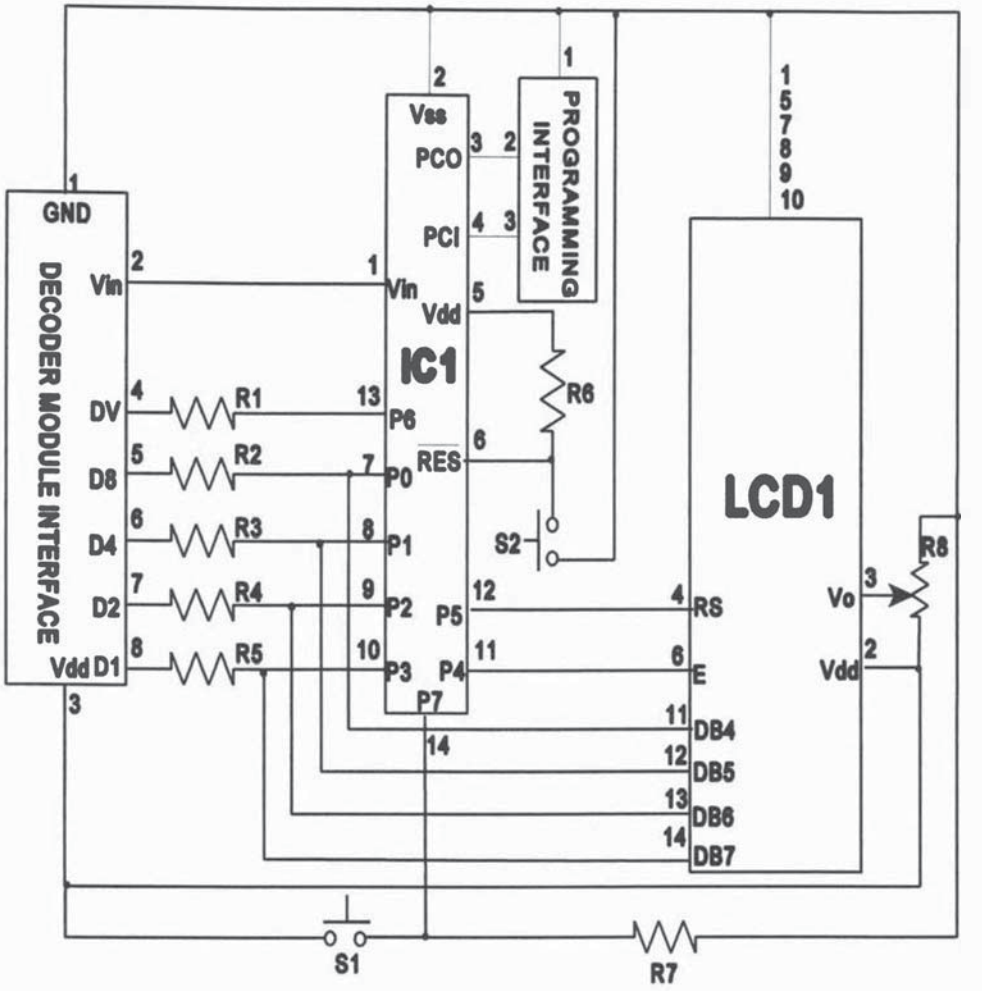


Figure 26. Schematic for LCD readout module.

Theory of Operation

Now you finally get to see why the modular design uses an eight-pin interface. Unlike its predecessors, this module uses all eight pins.

Interface pin 1 completes the ground circuit to the decoder module.

IC1 (the BASIC Stamp) uses the line voltage (+6–15 VDC) at interface pin 2 since it has its own five-volt regulator on board. The regulated five-volt output at pin 5 of IC1 comes in handy and eliminates the need for a PCB jumper to accommodate the reset circuit composed of S2, R6, and the reset line at pin 6 of IC1.

Interface pin 3 supplies a regulated +5 VDC for the mode-select circuit comprising S1, R7, and

the mode-select line at pin 14 of IC1. Interface pin 3 also supplies a regulated +5 VDC to the power supply (pin 2) of LCD1 and is used in the contrast adjustment circuit comprising R8 and the contrast adjustment line (pin 3) of LCD1.

Pin 4 of the interface brings the DV line onto the LCD display module for use by pin 13 of IC1. IC1 cycles in firmware waiting for pin 13 to be driven high by the DV line.

Interface pins 5 through 8 comprise the data bus, which carries the binary representation of the DTMF tone from the decoder module. When DV goes high, the firmware reads the binary representation at input pins 7 through 10 of IC1. Firmware then changes pins 7 through 10 to output pins and writes the corresponding decimal character to pins 11 through 14 of LCD1.

Resistors R2 through R5 ensure that IC1 has control of the data bus when writing to LCD1.

Pin 11 of IC1 toggles via firmware the enable line (pin 6) of LCD1 to tell the LCD to read the data bus.

Pin 12 of IC1 controls via firmware the register select line (pin 4) of LCD1, which tells the LCD if it is receiving data or a command.

Parts List

PART	VALUE	SOURCE	NOTES
(Big Stuff)			
IC1	BS1-IC	JDR/Digi-Key	BASIC Stamp
LCD1	16x1, +5 V	Digi-Key	Part #73-1012[1]
(Resistors—all 1/4 watt)			
R1–5	1 K	Radio Shack	
R6, 7	4.7 K	Radio Shack	
R8	10 K pot	Radio Shack	LCD contrast adjustment
R8[2]	330–4.7 K	Radio Shack	Alternative for nonadjustable contrast; 330-ohm for brighter display
(Hardware)			
S1, 2	PBNO	Digi-Key	Part #EG1828
14-conductor ribbon cable			Use color-coded starting on brown for easy pin-to-pin wiring
SIP socket	80 pin	Digi-Key	Part #ED7080-ND[3] can come in handy for this project
Jumper IC	16-pin DIP		(Optional) for easy jumpers to decoder module
3-pin header		JDR, Digi-Key	For programming port[4]
(4) 1-inch standoffs w/accompanying machine screws			

1. LCD must have Hitachi 44780 controller or equivalent. It must have a standard +5 VDC supply. (Marlin P. Jones & Associates has it for about $8.) The prototype was built with an OPTREX model DMC-16117A, aka Digi-Key Part No. 73-1012. The Sharp LM16155 also works well. Be warned that local electronics stores will probably overcharge you for this part.

2. A 4.7 K 1/4-watt resistor soldered between pins 1 and 3 on the LCD will provide a satisfactory contrast adjustment and eliminate the need for a potentiometer. Other values down to 330 ohms also work well.

3. A minimum of 14 pins of SIP socket will be needed for IC1. The rest of the SIP socket is for constructing the LCD

Procedure

1. Refer to the schematic, PCB layout, and stuffing diagram during assembly.
2. Be careful to observe the pin orientation of BS1 and LCD.
3. Use a 14-pin SIP for BS1.
4. Use a 14-pin SIP at the LCD.
5. Use a 14-pin SIP at the LCD interface port.
6. If you build your own LCD interface cable (discussed later in this section) be sure to observe the common color-coding scheme:

PIN	COLOR
1	Brown
2	Red
3	Orange
4	Yellow
5	Green
6	Blue
7	Violet
8	Gray
9	White
10	Black
11	Brown
12	Red
13	Orange
14	Yellow

7. Connect the LCD to the interface port via the homemade cable.
8. For best results use Digi-Key tact switches as suggested. The PCB is laid out for them.
9. When the LCD readout module is completed, interface it to a tested and functional decoder module.

Construction Tips

If you have not already done so, you should burn the decoder/LCD module "combo-board" for this project. You will be very pleased with the professional-looking finished product, which fits in the palm of your hand.

As with the decoder module, the LCD module's PCB is laid out for specific parts. These are S1, S2, and the LCD. For best results use the Digi-Key part numbers given.

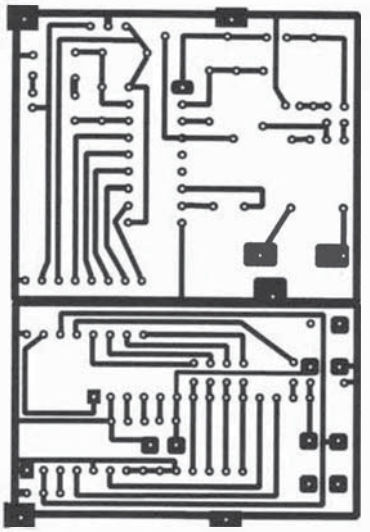


Figure 27. "Combo-board." If you've come this far, you might as well burn the whole board. If you only need the foil pattern for the LCD readout module, cut at the arrows and use the side marked "LCD." The extra solder pads at pins 2 and 6 of IC1 are from an older version and are not used in this project. Use a 1/32-inch drill bit or small Dremel bit to drill the holes.

cable, which is highly recommended. If you have some other 14-conductor cable you plan to use for the LCD, you do not need to get all the SIP socket and you won't need the ribbon cable.

4. For completeness, this module allows for in-circuit BASIC Stamp programming. If you have the BS1 carrier board, you can program the Stamp on the carrier board and then transfer it into the LCD readout module. If this is your plan, you do not need the three-pin header.

The LCD mounting holes will align with the four square pads on the outer edge of the combo-board. The prototype used 1-inch standoffs. If using metal standoffs, be sure you are not causing any shorts, especially at the input circuit where real estate is tight.

Unless you are insane, you will want to use 14 pins of SIP socket for IC1. Do you really want to desolder the Stamp every time you find a program bug? Plus, it's a great way to keep your Stamp available for other projects.

I also recommend building a cable for the LCD, unless you don't mind spending the money for one. You will need four 14-pin sections of SIP socket. Solder one 14-pin section to the PCB, another to the LCD. Solder 5 inches of ribbon cable between the two remaining sections. This takes a while but keeps your LCD free for other projects and experiments and makes for easier repair if the wires ever get frayed. For best results, tin the stranded wire before soldering to the SIP sockets. Also, use rainbow-coded wire and use brown for pin 1. This will make troubleshooting cable connections much easier. When the cable is complete, connect it between the SIP sockets already in place on the PCB and LCD, making sure the pin orientation is correct (another reason to use rainbow wire!).

Even if using the combo-board, you must remember the jumpers between the decoder module and the LCD readout module. Use 16-pin DIP socket and jumper IC for greatest versatility and easier future experimentation and expansion.

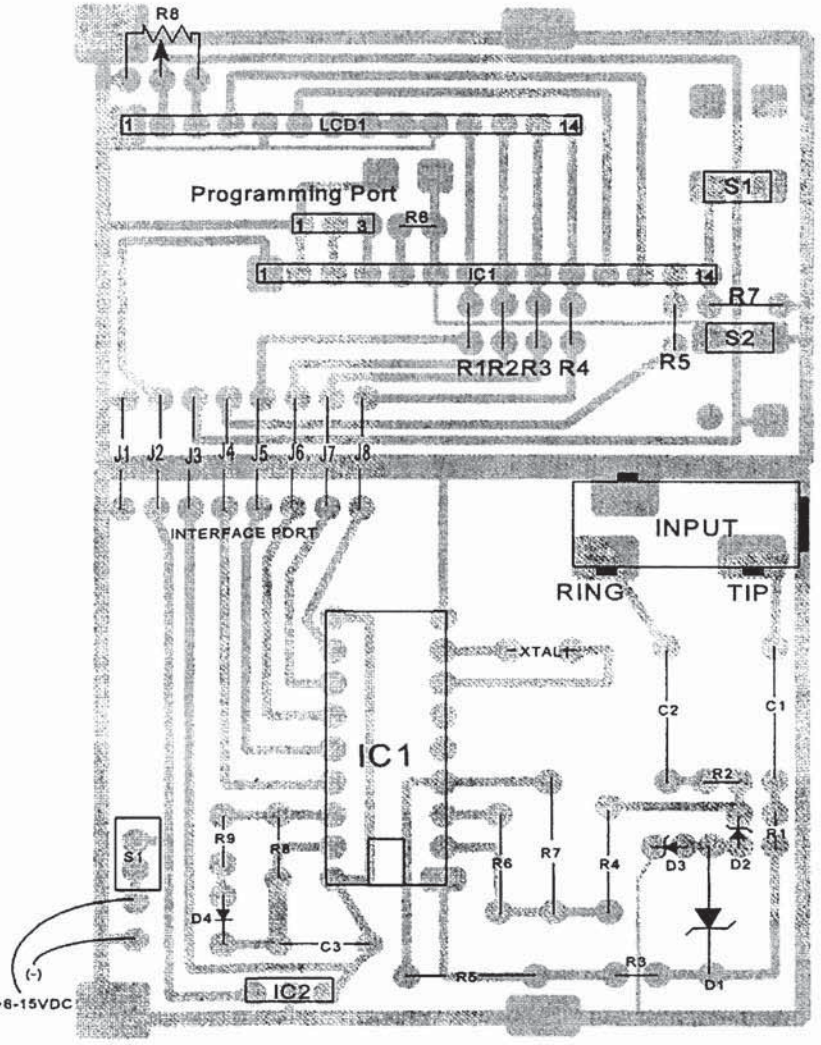
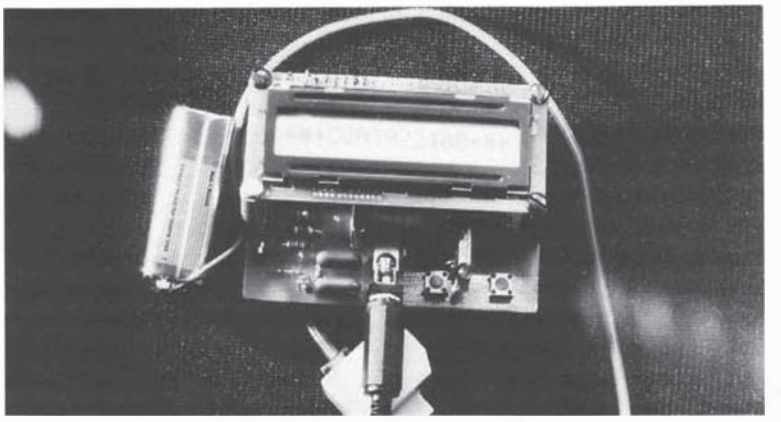


Figure 28. Don't forget the jumpers between the modules. If combo-board is used, J1 can be eliminated. Pilot holes on the LCD will line up with the four square pads on the PCB. Four standoffs (and eight matching machine screws) make for a sharp-looking finished product (see photo on next page). Drill square pads to accommodate machine screws.

Programming IC1

The BS1-IC chip (BASIC Stamp) must be loaded with the program in Listing 1 (see Appendix E). The program is the firmware that controls the flow of information from the decoder module to the LCD readout module. The



For best results, the decoder module and LCD readout module should be built onto a single PCB. With a little care and patience, you will have a professional-looking finished product!

first part of the program initializes the LCD. The rest of the program handles decoder module data, display, playback, and memory functions. This is a great project for anybody wishing to learn how to work with microprocessors.

The BS1 can be programmed from the PCB via the three-pin header. You will probably have less trouble, however, programming the BS1 from its carrier board. In either case, the BS1 must be properly oriented, powered up, and connected to a PC via the cable that comes with the programming package. If you're knowledgeable in PC interfacing, you can build your own cable (header pins 1, 2, and 3 correspond with parallel port pins 25, 11, and 2, respectively).

Start the BS1 programming software (Stamp.exe). It is best to do this from DOS because Windows can sometimes take over the communication ports in ways you can't readily control.

Procedure

1. Type in Listing 1, being sure not to make any mistakes. Listing 1 (reproduced in its entirety as Appendix E) is the firmware program for IC1. Every effort has been made to ensure that no typographical errors were introduced during the file conversion and editing process. Bugs could also be introduced when you type the program into your computer. To avoid errors, the exact program used for the prototype (DTMFPROG.BAS) is available for download at my Web site (see Appendix C for address).
2. Hit Alt-R to load the program into the BS1.
3. You will see the program load. A screen will pop up displaying the message, "Hit any key."
4. Hit any key.
5. Place the BS1 into the 14-pin SIP on the LCD readout module.
6. Turn power on at the decoder module (make sure both modules are interfaced!).
7. LCD should initialize to a blank screen with a cursor in the home position.
8. Connect the decoder module to a phone line and dial some digits.
9. The digits should appear on the LCD screen.
10. Depress reset switch S2.
11. LCD screen should clear, returning the cursor to home position.
12. Depress playback switch S1.
13. The numbers you dialed should read back out onto the display.

If BS1 Program Will Not Load . . .

1. Make sure Stamp.exe program is running from DOS and not from Windows.
2. Program BS1 from the carrier board and not from the PCB (to eliminate the possibility of PCB causing problems).

3. Make sure the BS1 programming cable is connected properly to the carrier board by matching the arrow on the cable with the arrow on the carrier board programming header. If you have built your own cable, make sure that pins 2, 3, and 4 of BS1 correspond with pins 25, 11, and 2 of the PC's parallel port.
4. Make sure BS1 programming cable is connected properly to the PC. The programming cable must be connected to a *parallel port*. You may need to temporarily disconnect your printer from the parallel port to accommodate the BS1's programming cable.
5. Make sure the BS1 is powered up. Connect a 9-volt battery to the carrier board.
6. If you get the message, "Hardware not found," recheck all of the above and then make sure the BS1 is properly seated in the carrier board. Also make sure the battery is not dead. Check for +5 VDC at pin 5 of the BS1. If pin 5 is less than +4 VDC, the battery is too weak to run the BS1. Replace it with a new battery.
7. If you get the error message, "EEPROM verify failed," keep trying. Your PC might be too fast or slow for the BS1. A repeated attempt may be successful. On one of my older computers, it sometimes takes up to eight tries to load a BS1 program if I have Windows running.
8. If nothing else works, try another computer, then another programming cable, and then finally a new BS1. If the new BS1 works, the old one is probably fried.

NOTE: Each binary representation of a DTMF tone is assigned a character by the firmware. This is accomplished with the command: EEPROM ("D84#206B195A3*7C"). When a DTMF tone is received, the firmware looks it up in a special EEPROM memory location, using the binary number as an offset. Since IC1 receives a mirror image of the actual binary code, the character assignments may seem random and incorrect. They are not. This was done intentionally for an easier PCB layout. You will note that the EEPROM offsets 0000, 0110, 1001, and 1111 correctly hold D, 6, 9, and C because the mirror image has no effect on binary palindromes.

Test Points

1. Make sure you have a good interface with the decoder module.
2. Check pin 1 (ground) of interface for zero VDC.
3. Check pin 2 of interface for supply voltage (+6 to +15 VDC).
4. Check pin 3 of interface for regulated +5 VDC.
5. Check for +6–15 VDC supply at pin 1 of IC1.
6. Check for regulated +5 VDC at pin 5 of IC1.
7. Check for zero VDC at pin 2 of IC1.
8. Check for +5 VDC at pin 2 of LCD.
9. Check for zero VDC at pin 1 of LCD.

If any of the above values do not check out, disconnect power immediately and recheck your work!

10. Check for corresponding 8870 output latch (pins 10 through 13) values at pins 7 through 10 of IC1.
11. Check for +5 VDC at pin 13 (data valid) of IC1 while depressing telephone key.
12. Check for 0 VDC at pin 13 of IC1 when key is released.
13. Check pin 14 of IC1 for 0 VDC (it should be tied low by R7).
14. Check pin 14 of IC1 while depressing S1. It should go to +5 VDC.
15. Check pin 6 of IC1 for +5 VDC (it should be tied high by R6).
16. Check pin 6 of IC1 while depressing S2. It should go to zero VDC.
17. Check pins 1, 5, 7, 8, 9, and 10 of LCD for zero VDC.
18. Check pins 11 through 14 of LCD for shorts or open traces.

19. Check continuity from pin 11 of IC1 to pin 6 of LCD.
20. Check continuity from pin 12 of IC1 to pin 4 of LCD.

Troubleshooting

If the LCD does not operate, verify the proper orientation of IC1 and LCD. Verify the interface with the decoder module. Verify all data connections. Check over your work, especially the 14-pin interface cable between the LCD and PCB. Verify pin-to-pin continuity and check for shorts between adjacent pins.

If the LCD is completely dark, it is probably not receiving power or the contrast resistance may be too high. Eliminate the potentiometer and solder a 4.7 K resistor between pin 3 and pin 1 (ground) of the LCD during testing.

If the LCD comes on but half of it is dark and the other half is light, it is not properly initialized. Make sure you have the right kind of LCD. It should be one row of 16 characters. If in doubt, use the part the number specified. Make sure Listing 1 has been properly typed into the Stamp compiler. Be sure the initialization phase of the BS1 program is correct. Also, check the LCD_WRITE subroutine for mistakes.

Use

At power up or reset, IC1 initializes LCD1 with a firmware initialization scheme. The LCD is placed in four-bit mode, cleared, and a cursor appears in the first character block. IC1 then waits for a DTMF tone.

When a DTMF tone is received, that character is then written to LCD1 and stored in the EEPROM onboard IC1. LCD1 immediately displays the character on screen and advances the cursor. IC1 waits for the next tone and the process repeats.

There are two modes of operation: play and record. At power up or reset, the unit is automatically placed in record mode and can save up to 16 digits in nonvolatile EEPROM. After 16 digits, the unit resets.

Holding S1 plays back the recorded tones.

When finished playing back tones, you should hit the reset switch so that the LCD screen corresponds with the EEPROM memory locations of any new tones received. Failure to do this, however, will not harm the unit.

Notes

The prototype was built on the same PCB as the decoder module (see photo on page 39). The design allowed proper spacing for a 16-pin DIP socket to straddle the boundaries of the two PCB layouts. A 16-pin jumper IC was placed in the socket to complete the jumper arrangement while allowing an easy disconnect to test other modules, prototypes, and future ideas.

The BS1-IC is not cheap. It is, however, easy to use and program, and many serious hobbyists already own one, which is why I chose to incorporate it into this design. The enterprising electronics engineers in our readership may wish to design their own microcontroller circuit for the LCD module and plug it directly into the 14-pin port intended for IC1. Since other readers may be interested in reviewing such circuits, please don't hesitate to share them with us. (See Appendix C if you wish to share your design for possible use on the author's Web site or to receive updates to this text.)

Alternative Uses

A DTMF decoder can be converted to a telephone accountant to keep track of your long-distance calls, or it can be used in conjunction with your scanner or ham radio to decode beeps heard on your local repeater.

Tricking the TelCo

As we've seen, a DTMF decoder is certainly a nice device to have. But what if you don't own one and you're not quite ready to brew your own? Contrary to what you may have heard, DTMF tones can be decoded without a DTMF decoder, but this requires some imagination.

They say that necessity is the mother of invention, right? Well, one time I had a desperate need for a DTMF decoder but no immediate means of procuring one. So after some thought, I devised a way to decode DTMF tones with the help of my local telephone company.

I realized that, although I did not own a DTMF decoder myself, I was sure the telephone company owned several hundred thousand. I also knew that my telephone contained a DTMF generator to facilitate Touch-Tone dialing. Certainly, I thought, there must be a way to make use of what already exists in the telephone equipment.

The only practical way to use my method is to have the DTMF tones recorded on tape (or some other medium such as your PC). What was I doing with DTMF tones on tape? I was just experimenting, of course. I assure all federal authorities reading this book that these tones were not recorded from a certain female's cordless phone during the course of a four-hour surveillance gig for which I was paid $600. I further certify that the $600 did not come from a certain out-of-state male consort of this female who'd been wondering whether he should propose marriage to her, which he eventually did not. My, how the industry is changing . . .

So, get some DTMF tones on tape. If you are unsure how to do this, see the following section.

Use your own phone and dial your own number and you probably won't be breaking any important laws. Now, using the same tape deck, play the tape back through the telephone receiver, being sure to use the microphone (speaking) end of the receiver. You may have to experiment with different volume levels and microphone distances before your friendly telephone company will properly process the recorded signal. To prevent frequency fluctuations, allow plenty of time for the tape to get up to speed when you are recording and playing the tones. Then, when you've properly balanced all these requirements, you will get a busy signal (assuming you dialed your own phone number as suggested).

Please, please, *please* don't make the embarrassing mistake of using this method to decode a phone number recorded during a surveillance gig—only to have it work flawlessly—in which case your subject's consort (friend, lover, drug partner, or worse) answers the phone wondering exactly who the hell you are. If this angry lover or drug dealer happens to have Caller ID, he will then, in fact, know exactly who the hell you are—and where you live. . . . Well, this could amount to more than just embarrassment at this point. Savvy?

Now, assuming you've been properly authorized to record a telephone conversation in which the party conveniently dialed several phone numbers, the proper method for decoding DTMF tones off of a surveillance tape follows.

If the number is a long-distance one (11 digits), play the first seven recorded tones into the receiver. In most cases, this will be a "1" followed by the area code followed by the exchange. This requires you to be ready to stop the tape immediately after the seventh tone, so be ready. Then, manually press 0-0-0-0. If you are successful, you should get a message like, "The number you have reached, area code X-X-X-5-5-5-0-0-0-0, is not in service at this time." Do you see the beauty in this? Now you have the area code and exchange! Not bad for a dude or dudette who does not own a DTMF decoder!

To get the last four numbers, manually dial 1, then a big city area code (such as for Los Angeles, Boston, Chicago, or New York), then play the first three of the last four recorded tones, and then manually dial 0-0-0-0. If you are lucky, these digits will represent an actual exchange in the area code, and the TelCo message will uncover three more digits for you. Then repeat this process for the last three digits of the phone number.

You can also decode any recorded number one digit at a time with the 0-0-0-0 method. This involves becoming familiar with your local exchanges. If you know, for instance, that your area code has filled up exchanges 340–349, then you can dial 34, then play one recorded tone, then dial 0-0-0-0 and you should get a message like, "The number you have reached 332-0000 is not in service at this time." Now you know that the number from the tape is a "2." If you are daring, you can run more of the recorded numbers through and hope you reach a phone number that is not in service. I would suggest not being this daring from your home phone.

The foregoing examples are just a few ways to trick the TelCo into decoding DTMF tones for you. Adding your own creativity to the above information, you should have no problem coming up with a customized method more suited to your geographic area.

How to Get DTMF Tones on Tape

Differences in tape speed will affect the actual frequency of the tones. The general rule is, if you play the tape at half-speed the frequency will be reduced by one octave. When using the above decoding method, it is very important that variations from recording speed to playback speed are nearly nil. This is why it's best to record and play back on the same tape deck. Variations from one machine to another will wreak havoc with this decoding process.

One way to eliminate the tape speed problem is to record the tones onto digital audio tape or some other form of digital recording. Recording tones onto your computer's hard drive (using appropriate software) will also do the trick. You musicians in the audience will also be aware of a device called a "sampler." This machine will also work nicely. In any case, when recording digitally, it is important to be sure that your "sample rate" is sufficient. In general, if you choose the highest setting for whatever device you are using, you should not have a problem. This rule may not apply to outdated machines.

Serendipity—No Decoder Needed!

What do you do when DTMF tones start streaming into your scanner, but—oh, my God—you don't yet own a decoder? Do you block your ears? Do you turn the volume down and sniffle? Do you bury your head in your arms and say, "Look away, I'm hideous?"

Well, one time this happened to me (can you believe it?). The DTMF tones were streaming in, and I was kicking myself for being without my decoder. Somewhere around the third kick, I heard a disharmonious, high-pitched, three-tone arpeggio followed by the TelCo operator saying, "The number you have reached, 555-765-4321, is being serviced. No further information is available for 555 . . ." Well, the numbers have been changed to protect the dubiously innocent, and I can't remember exactly what the recording said, but you get the idea.

Another time, long before I ever built my first decoder, I had a subject who had a certain consort with an unlisted number that I really, really needed to get my grubby stubs on. During a surveillance, my subject twice attempted to dial this particular consort and on both occasions apparently got the wrong number (there was a lot of grumbling, swearing, and muttering under his breath to that effect). After a minute, he clicked his cordless back on and I heard him mutter, "I got an idea . . ." The next number he dialed gave him this recorded TelCo message: "The number you have dialed, 555-123-4567, has been changed. The new number is 555-456-7890." My subject apparently figured that the number change was recent enough to trigger the TelCo message. Good idea. I do the same thing every time my sister moves—but not from a cordless phone!

Summary

The modular DTMF decoder system presented in this chapter allows the novice to start with a simple decoder. The possibility for expanding to a more sophisticated design is left open. When that

time comes, there will be no need to completely rebuild the project.

This system allows advanced hobbyists to jump right in and build a DTMF decoder with LCD readout. The modular design also leaves open the possibility of including a memory buffer or other modification without having to completely redesign the circuit.

I've demonstrated that decoding DTMF tones can, in fact, be done by someone who does not own a DTMF decoder. The TelCo-tricking method is a great place for the novice to wet his or her feet. It's also useful in a pinch when the operative is without his DTMF decoder.

Electronics hobbyists will benefit from examining, building, and using these designs to better understand electronics theory and implementation. The LCD readout project propels the hobbyist into the fascinating world of using embedded controllers and firmware to enhance project and prototype designs.

Law enforcement officials and private investigators, with valid court-issued warrants, can use the designs and tricks in this chapter for surveillance operations. Police departments in smaller jurisdictions often operate on shoestring budgets; they will surely appreciate and benefit from the low cost of brewing their own surveillance equipment.

CHAPTER 4

BUILDING A RED BOX

I suppose the quickest instructions would be to cut six squares of plywood, glue them together in the form of a cube, and paint it red. Only we're not talking about that kind of red box.

"Red box" is slang for a device that generates the electronic signal produced by a pay phone when a coin is dropped into it. You hold the red box up to the pay phone's mouthpiece, press the friendly button that generates the nice beeps, and then place your call as normal. The first illegal device of this nature confiscated by the authorities was red; hence, the name.

People that endeavor to hack into and abuse telephone networks are known collectively as "fone phreaks." Fone phreaks like to changz the spelling and capitalization of wOrDz, eZpecIaLLy on the Internet. I won't do this to you, but I've always liked the word "phreak," so I may use it from time to time. The only real problem with fone phreaking is that the telephone company gets ripped off. Oh, yeah, and it's probably illegal.

There are only a few ways to come into possession of a red box:

- Buy one on the black market.
- Build one from scratch.
- Modify a Pocket Tone Dialer.

Buying on the black market: This option is difficult, dangerous, expensive, and possibly illegal.

Building from scratch: Not a bad idea. I've never done it, personally. The main reason for this will become clear in a moment.

Modify a Tone Dialer: In Chapter 5, you will learn how law enforcement professionals (and others) crack answering machine codes. You will also learn how this process is greatly simplified by using a Radio Shack Pocket Tone Dialer with 33-number memory. You may then feel the need to run out and buy a Tone Dialer. If you also become interested in red boxing, you may feel the need to own two Tone Dialers, one for each purpose. "But, gee, these little suckers are expensive, and I don't like giving my money to corporate America. Wouldn't it be really nifty if I could use one Tone Dialer for both dubious purposes? Isn't there a way to do this?"

C'mon! You know I'd never leave all'y'all hangin'. I don't like to give money to corporate America either. What if 1,000,000 people read this book and only a mere 10 percent of them decide to phreak answering machines and build a red box? At $25 per Tone Dialer times two, that's $5,000,000 gross for Tandy Corporation. With an average state sales tax of 5 percent, that's another $250,000 to state governments around the globe. This rubs me the wrong way, and I feel it's my duty to cut these figures in half or, in fact, in thirds. So, what follows are step-by-step instructions for modifying a Pocket Tone Dialer with 33-number memory. When completed, this Tone Dialer will actually serve three purposes: "standard mode" tone dialing; "phreak mode" red box dialing; and finally, as you will learn in the next chapter, answering machine hacking, cracking, and hijacking.

PARTS LIST

PART	VALUE	SOURCE	NOTES
Tone Dialer	33-number memory	Radio Shack	Catalog item #43-146
XTAL-1	6.5536 MHz*	Digi-Key	Part #X018
S1	SPDT (slide switch)	Digi-Key	Part #EG1901
Hookup wire	Small gauge	Radio Shack	Smallest gauge you can comfortably work with. You must be able to solder this wire. Do not get wire-wrap type!

* You may also use a 6.5 MHz crystal.

The Radio Shack Tone Dialer in the above parts list (catalog item #43-146) has recently been modified by Tandy Corporation to trick phone phreaks into thinking that red boxing with its product is no longer an option. If the phreak does attempt to modify the dialer into a red box, the new design makes it very difficult. Because I have nothing but the utmost respect and admiration for my readers, the procedure below was engineered, performed, and tested on a recently purchased Tone Dialer in order to

- prove that it can still be done;
- give Tandy Corporation one "In Your Face!"; and
- demonstrate the new procedure to the public.

If you happen to work for, own, or just respect Tandy Corporation, please bear in mind that the "In Your Face!" is meant only in the friendliest of manners and not in the pejorative. I have given, directly and indirectly, several lifetimes' worth of business to Tandy Corporation (and have given my name and address—real, imagined, and made up—to its Radio Shack clerks countless times).

To the very best of my knowledge, a procedure for phreaking these new Tone Dialers has hitherto not been published. Here, my friends, is an honest-to-goodness, hot off the press, in their faces, knock 'em dead, tell-your-friends-tell-your-neighbors, honest-to-goodness (did I already say that?) GIMME . . .

PROCEDURE

(Refer to Figure 29 on page 61.) Please note that all locating instructions from steps 6 through 27, such as "upper right," "center," or "second solder pad down" are with respect to the orientation of the Tone Dialer as depicted in Figure 29 and NOT as you would normally be looking at it.

I. Gain Access

1. Place Tone Dialer face down on soft cloth.
2. Remove cover of battery compartment.
3. Remove batteries (optional).
4. Using a sharp utility knife, cut a 1/8 x 5/8-inch rectangular hole between the two screws below the battery compartment as shown in Figure 29. This space will house the new crystal.
5. Remove the six screws that fasten the rear panel to the front: two below the battery compartment, two above the battery compartment, and two above the speaker. These screws are not all the same size, so be sure to note their proper location for reassembly. (The bottom screws are smaller.)
6. With speaker on the right and battery compartment on the left, carefully pry the rear panel of the Tone Dialer from the front panel. Once it is loose, flip the rear panel away from you so as not to yank the four speaker wires. Internal wiring is

just long enough so the rear panel can be flipped all the way back for convenience.

7. The two slide switches are now loose at the bottom of the PCB. Put these aside for reassembly.

II. Make Electrical Connections

8. Locate the 3.58 MHz ceramic resonator near the top of the circuit board.
9. Cut the left leg of the resonator in half.
10. Desolder the bottom half of the cut left leg from the PCB and discard. A "solder sucker" is helpful here.
11. Solder one end of a 2-inch length of small gauge wire to the left leg of the resonator.
12. Solder the other end of the 2-inch wire to one side of the miniature SPDT slide switch.
13. Solder one end of another 2-inch wire to the center of the SPDT slide switch.
14. Solder the other end of that 2-inch wire to the solder pad where the resonator's left leg was previously connected.
15. Solder a 5-inch length of wire to the other end of the SPDT slider.
16. Slide a 1-inch piece of 1/16-inch shrink tubing over the 5-inch wire.
17. Solder the other end of the 5-inch wire to one leg of the 6.5536 MHz crystal.
18. Slide the shrink tubing over the exposed lead of the crystal and shrink it with a heat gun or heat from your soldering iron.
19. Solder a 4-inch length of wire to the other leg of the crystal.
20. Slide a 1-inch piece of 1/16-inch shrink tubing over the wire covering the exposed lead of the crystal and shrink it in place.
21. Solder the other end of the wire to the other leg of the 3.58 MHz ceramic resonator.
22. For proper orientation, position the Tone Dialer per step 6 and refer to Figure 29. Using a sharp utility knife, hacksaw, or nibbling tool, cut a 1/2-inch notch in the side of the rear panel beginning just to the left of the screw guide nearest the speaker connections (opposite the side of the half-moon slide switch cutouts). This is where the slide switch will exit the enclosure.

III. Make Space for Switch

23. Remove the 2.2 µF electrolytic capacitor from the upper right corner of the PCB.
24. Solder the positive leg of that capacitor to the second solder pad down from the top left. Note that this pad is electrically connected to the capacitor's previous location.
25. Solder the negative leg (marked "minus") of the capacitor to the second solder pad to the left of (and about 1/8 inch below) the solder pad referenced in step 24. You will need a 1/2-inch jumper wire to make this connection. Shrink tube the jumper if possible. Note that this location is electrically connected to the capacitor's previous location.

IV. Reassemble

26. Place a small square of electrical tape over the speaker wire pads (both ends), 3.58 MHz resonator connections, electrolytic capacitor (from above procedure), and anywhere else that might need insulating.
27. The two wires from the 6.5536 MHz crystal may be routed around the upper left screw guide and then pushed gently below the top side of the PCB (as oriented in Figure 29).
28. You may need to cut some of the plastic casing away to get everything to fit, especially if you used heavy-gauge wire. Cutting some plastic from around the screw guide will aid in stuffing the wires behind it. Cutting the plastic "tongue" of the front panel by the crystal wires and screw guide will give the wires some breathing room and help the enclosure to snap back in place.
29. Replace the two slide switches metal side down (these were set aside in step 7).
30. Without using excessive force, snap the

enclosure together. This is a little tricky because you have to be sure the two slide switches, your SPDT switch, the crystal, and all wiring are in place. The complete lack of real estate inside the Tone Dialer means that extra care must be used on this step.

31. Replace the six screws. If any screw does not fit correctly, redo step 30. The enclosure must be properly screwed together or slide switches will not be in contact with the PCB and will not function.
32. Replace batteries (if removed in step 3).
33. Replace cover to battery compartment. You may need to push the crystal down first.
34. Make sure all switches are in place and working.

Test

35. Slide "Store/Dial" switch to "Dial."
36. Slide power switch to "On."
37. Press the "5" key and note the pitch of the tone.
38. Slide your SPDT switch to the opposite position.
39. Press the "5" key again and note pitch.
40. The switch position that makes the lower pitch is the "standard mode" position. We will refer to the opposite position as "phreak mode." If you've followed the wiring diagram in Figure 29, the "up" position is phreak mode.
41. Switch Tone Dialer to "standard mode."
42. Holding the padded speaker of the Tone Dialer firmly against the mouthpiece of a standard telephone, dial that phone's number. You should hear a busy signal, indicating that the DTMF tones were sent properly to the central office.
43. If steps 37 through 42 don't go as planned, recheck your work, noting the special troubleshooting concerns listed below.

TROUBLESHOOTING

- *No power*:
  - —Screws may not be seated properly (causing poor slide switch contact with PCB).
  - —Slide switches are in upside down.
  - —Battery polarity is incorrect,
  - —Battery lead was disconnected during procedure.
  - —Batteries are dead.
- *No sound*:
  - —SPDT switch is in middle position (must be either up or down).
  - —Speaker wire was disconnected during procedure.
  - —Crystal wiring is shorted or open.
  - —SPDT switch is wired incorrectly.
- *Tones do not signal central office in standard mode*:
  - —SPDT is set to wrong position.
  - —Tone dialer is not seated properly against telephone mouthpiece.
  - —Phone is not standard (some cordless phones won't work well).
  - —Mouthpiece is muted (some pay phones)
  - —There is a cracked or squished 3.58 MHz resonator (rare)
- *Tones do not signal central office in phreak mode*:
  - —SPDT is set to wrong position.
  - —Tone Dialer is not seated properly. against telephone mouthpiece.
  - —A TelCo security device is present in pay phone (see below).
  - —The 6.5536 MHz crystal is cracked. (very rare)

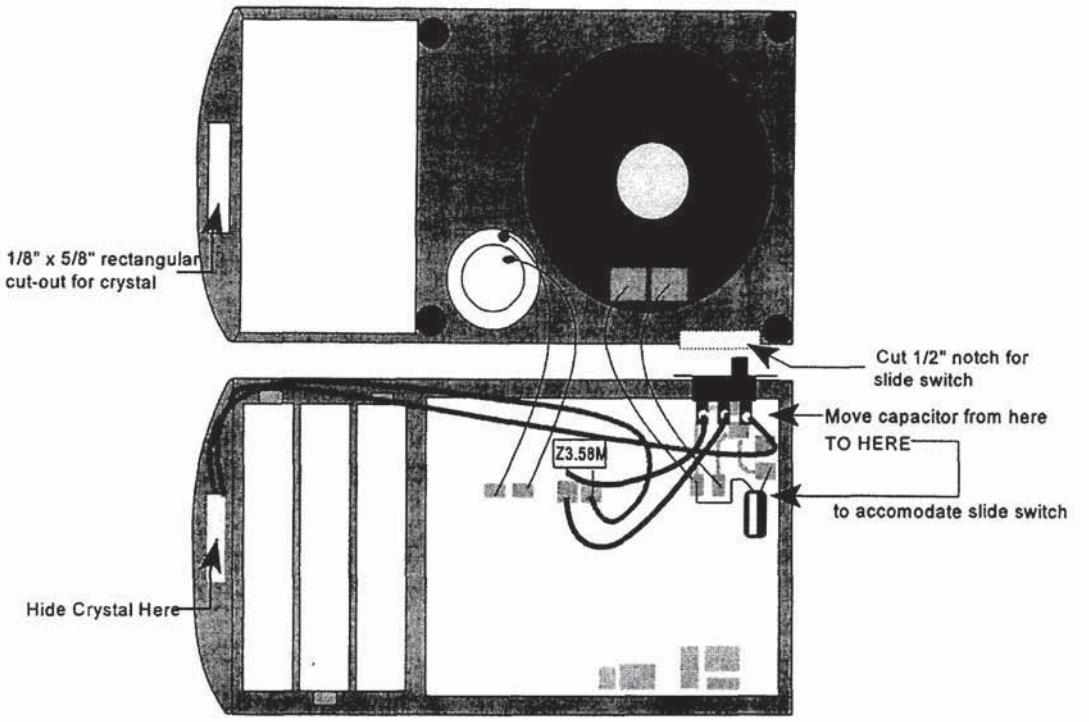
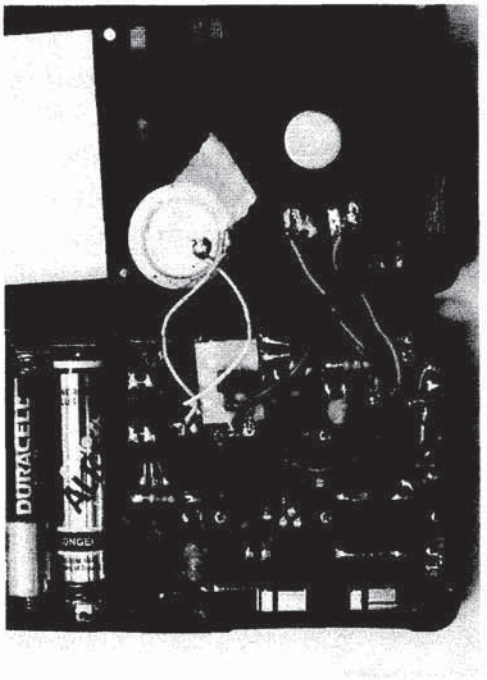
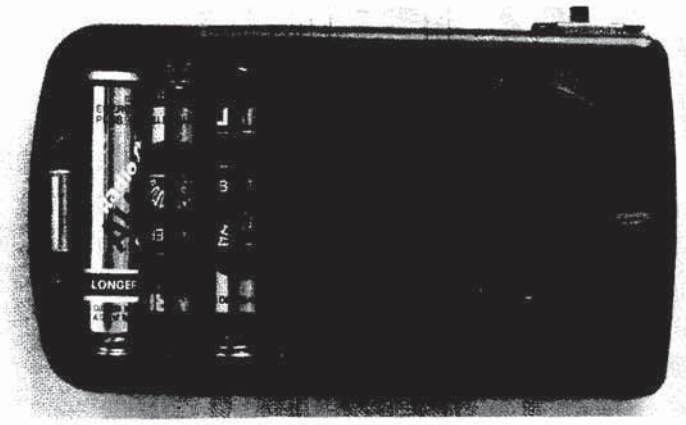


Figure 29. Use this illustration to determine the location of critical Tone Dialer components.



Tone Dialer rewiring. Note the location of new SPDT switch and routing of wires. You only need to clip the left leg of the ceramic resonator. There's no need to remove it.



Placement of crystal. Due to lack of real estate, the new crystal must be hidden in the battery compartment. Battery compartment cover operates normally with crystal in place.

Theory of Operation

The 6.5536 MHz crystal alters two important electrical characteristics of the Tone Dialer, the first being that the higher reference frequency produces higher tones. Go ahead and try it. With the dialer switched to "standard mode," press a key. Now, switch the dialer to "phreak mode" and press the same key. You will notice that the pitch is higher in phreak mode. Not only is it higher, but the phreak mode star (*) key happens to be the same pitch as a nickel falling into a pay phone. In actuality, the pitch is not exact, but it's so close that TelCo equipment accepts it.

To demonstrate the second electrical characteristic, the Tone Dialer must first be programmed.

I. Program P1

1. Turn Tone Dialer ON.
2. Slide DIAL/STORE switch to STORE.
3. Press MEMORY.
4. Press the star (*) key.
5. Press MEMORY.
6. Press P1 (actually you could use any memory location).
7. Wait for Tone Dialer to give confirmation beep.

II. Program P2

8. Press MEMORY.
9. Press the star key twice (*, *) .
10. Press MEMORY.
11. Press P2.
12. Wait for Tone Dialer to give confirmation beep.

III. Program P3

13. Press MEMORY.
14. Press the star key five times (*, *, *, *, *).
15. Press MEMORY.
16. Press P3.
17. Wait for Tone Dialer to give confirmation beep.
18. Slide the DIAL/STORE switch to DIAL.

IV. Test

19. With the dialer in standard mode, press P2.
20. You will hear two consecutive star key presses.
21. With the dialer in phreak mode, press P2.

Notice anything different? Yes, well, we already said that the pitch is higher in phreak mode, but did you notice anything else? That's right. *The memory output is faster.* You hear the beeps in rapid succession, just as when you drop a dime into a pay phone. This is because the memory output also uses the crystal as a reference frequency. You're using a higher frequency crystal, so the tones are played back faster.

Each beep represents a nickel. If you only need a nickel, you can press the star key, but it's probably best if you only use the P1 key, as the staccato effect more accurately mimics what goes on when you drop money into a pay

phone. This is harder to replicate with manual key presses.

Red Boxing: A Dying Phenomenon?

Now, before you run out the door to field-test your red box, there are a few things you need to know about the red boxing pastime. First, it's probably illegal. So, it's best if you wait for Congress to pass a law declaring red boxing a perfectly legal practice. Second, telephone companies, for some unfathomable reason, do not like to be ripped off. Thus, they have implemented some countermeasures against would-be red boxers.

The first and most obvious countermeasure is the dreaded muted pay phone, or *redboxicus dontbotherus* as it is called in Latin. Drive around some day and blow into pay phones. Don't laugh. I had to do this during the research phase of writing this book. You will notice with some pay phones that your breath does not echo into the earpiece. This is because the mouthpiece (microphone) is muted until you put money in the phone and the call is connected. This means that if you hold your red box up to the mouthpiece and try to serenade the phone company with some fancy money-generating music, it will not hear your overture. A nice lady will come on the phone and say in a friendly recorded voice, "Please deposit $3.20 for the first two minutes." She will keep saying this no matter how much you try to phreak her out. In short, your red box will not work on this pay phone.

Then there's the dreaded nonmuted pay phone that still won't work because it's picky. As a person knowledgeable in electronics, I have my suspicions about why these pay phones don't like red boxes. I figure it's best not to publish them, though. If I happen to be wrong, why give the phone company any good ideas?

If you encounter either of the above, try depositing a nickel first. Sometimes that does the trick. Also, keep in mind that all company-owned coin-operated telephones (COCOTs) are not red box friendly. These are the pay phones you see outside convenience stores, and they are not owned by the phone company.

Then we have the nonmuted pay phone that is not too picky, aka the "friendly phone," or *redboxicus dialawayatus*, if you prefer the Latin term. The friendly phone likes red boxes and is very forgiving. You need to find as many of these phones as possible because the friendly phone companies are on to red boxing, and soon it will be a thing of the past, like blue boxing (a story for another time). A hint: The more rural the location, the better chance you have of finding a friendly phone. Don't worry, though. There's still plenty of them around. When you find one, do everything in your power to protect it. Don't let the local kids rip the cord out because once the TelCo comes to repair it, you can betcha the repair dude has a van full of muting gadgets and it's bye-bye friendly phone, hello 21st century.

Spotting a Friendly Phone

If you attend a phreak show, you will hear some general, often unconfirmed, rules regarding friendly phones and which companies have more of them. Phone companies seem to change names and buy each other out on a daily basis, and I hate to publish such ephemeral information. That said, I have heard that Bell and GTE pay phones are the friendliest. Take it as you will.

Friendly Phone Etiquette

Even friendly phones have their standards, you know. First of all, most of them will require at least a nickel so any TelCo "ground test" will confirm that some money has actually been deposited. Box the "dimes" in too fast and a friendly phone lady will come on the line and ask, "May I help you?" In friendly-phone-ese this translates into, "I don't think any human could pop dimes into a pay phone that fast, so I'm getting suspicious about your intentions while also hedging my bet in the event it's actually our equipment malfunctioning, which is damn near impossible in this day and age."

If this happens, you can pretty much handle it any way you want. The phone lady doesn't have a red button that alerts the FBI to

your potentially illegal activity at 1125 Redbox Lane pay phone #113011 . . . yet. You could simply hang up the phone and go elsewhere. Or you could even say, "I ran out of change, but I thought I put in enough. How much more do I need? Ooops wait a minute, here's another dime." Put in a real dime and say, "Does that do it? Did you get that? Hello? Hello? Heeeeelloooo????" in a high-pitched, confused voice that trails off. Or whatever. You could even say, "I built this device that's supposed to allow me to make free phone calls from pay phones. Is it working?" Just to see what happens. Or you could just drop some "nickels," "dimes," and "quarters" in with your red box. Believe it or not, this often works best. The phone lady can't tell the difference (usually) between 5 pulses per second (pps) and 12 pps. Most phone ladies don't even know to listen for such a thing. Careful, though, I've dealt with savvy phoneladies, too. They say the darndest things! Oh, and they will disconnect your call. Sometimes they try to scare you by saying, "Hold on, I'll put you through to the FBI," and other attempts to scare us "kids" off the line. Right!

Okay, so I like to tease the phone company. Occasionally, people are arrested for red boxing, though. And if you think the operator is on to you, it's best to go elsewhere. Some operators can record your routing information to be used as evidence in court. So, don't use the same phone over and over. Don't dare the operators, if the occasion should arise. Don't use phones in such a way that a path is led right to your door (such as making several red box calls during your 600-mile trip home and then getting greedy and using the phone across the street).

The best way to drop dimes into a friendly phone, without attracting too much attention to yourself, is to follow these steps:

1. Wait for Congress to pass a law declaring red boxing a perfectly legal pastime.
2. Find a friendly phone.
3. Dial a long-distance number.
4. Wait for the friendly phone lady to say, "Please deposit $.65 for the first two minutes."
5. Deposit an obligatory nickel.
6. Wait for the friendly phonelady to say, "Please deposit $.60 for the first two minutes."
7. Press P1 and P2 at irregular intervals until you've "paid" enough for your call. Remember, you're trying to act like a real person searching for change and taking the time to put it in the phone. You don't want to trip any flags on the TelCo computer. It can't hurt to throw in a couple more real nickels to break things up.
8. Wait for the friendly phone lady to say, "Thank you. You have 5 cents credit" (or whatever).
9. Proceed with your call and don't act suspiciously. For instance, don't yell out to the public, "Hey everybody, I'm ripping off the phone company!"

You may have noticed that this procedure conspicuously avoids use of the red box "quarter." There is a reason for this . . .

Pay Phone Operation

When you put a real nickel into a pay phone, it signals the central office by sending a special DTMF tone. The DTMF tone is made up of a 1,700 Hz tone and a 2,200 Hz tone. The tone sent by the pay phone is of a certain duration. When you put a dime into a pay phone the same DTMF tone is sent to the central office, except it is out-pulsed twice (two nickels = one dime). Again, the duration of each tone is roughly the same as a nickel, and they are out-pulsed at about 12 per second. A dime tone sounds for about one-fifth of a second. When you put a quarter into a pay phone the same DTMF tone is out-pulsed five times. The tone durations and pulses are slightly faster, though, at about 17 pulses per second.

The Radio Shack Tone Dialer red box out-pulses the tones at about 9 to 10 pps. The slight discrepancy does not seem to bother most friendly phones. More and more, however, I've

noticed that red box quarters will draw a live operator to a friendly phone where red box nickels and dimes won't. The only conclusion I can draw is that the phone companies are beginning to implement precision standards that are breached by the exaggerated out-pulse discrepancy of red box quarters. Now, don't go posting this information on Usenet groups just yet. We do not want to spread unconfirmed rumors. You must realize that this is purely conjecture on my part. It's just a theory I formed to explain a problem I've been having with red box quarters. This is a recent problem and calls for more observation before a more solid conclusion can be reached. I would suggest you monitor Usenet groups such as alt.phreaks and alt.2600 to see whether any other phreaks are having similar problems with red box quarters.

The other thing to consider is that our red box DTMF tone is not really a 1,700 and 2,200 Hz tone. Look at the DTMF Tone Matrix again in Figure 13 on page 34. Note that the frequencies for the "*" key are 941 and 1,209. If these frequencies are generated by a 3.579545 MHz crystal and a 6.5536 MHz crystal is 183 percent faster, we can calculate the modified frequencies of a red box "*" key.

941 x 1.83 = 1,722 Hz
1,208 x 1.83 = 2,211 Hz

Notice that the frequencies are slightly off. The TelCo is expecting 1,700 to 2,200, and we're sending them 2,211 to 1,722. Perhaps this discrepancy, combined with the out-pulse discrepancy, is being exploited by telephone companies to discriminate against red boxers. Again, food for thought. Keep an eye out and be sure to share information with Usenet groups, phreak clubs, and your local anarchist. If the TelCo is beginning to implement sensitive equipment to look for these discrepancies, we phreaks and red boxers will surely have to answer this. One quick suggestion is to use a 6.5000 MHz crystal instead of a 6.5536 MHz crystal if you can find one. This will get you a little closer to the correct frequencies. Some say it works better; others say there's no difference.

Tone Dialer Alternatives

Recording actual nickel, dime, and quarter tones from a pay phone will eliminate out-pulse and frequency discrepancies, provided that the recording is digital and the sample rate is high enough. You can use a digital Dictaphone. I've also heard that you can use those Hallmark Greeting Cards that were around for a while. You know, the ones where you can record a personalized message. Radio Shack sells a suction-cup-type telephone transducer that will assist you in the recording process. I've never done this, so you may wish to look for tips on the World Wide Web, newsgroups, or other nonmainstream publishing sources.

Analog tape recorders will probably work, too, though probably not dependably. A decent-quality microcassette recorder may do the trick if you use the same one to record and play back the tones. Remember the caveats from the "How to Get DTMF Tones on Tape" section of Chapter 3? The same principles apply here.

Legal Uses

A red box cannot be converted to anything except a jail sentence. Therefore, after building this gizmo, it can only be tested with an oscilloscope (field-testing is currently illegal). Then, unfortunately, it must be destroyed.

That's It, Jack

Well, that's all there is to it. Take your time, follow the instructions and when you're done, use an oscilloscope to test your work. Please, whatever you do, don't hassle the folks at your local phone company.

Since the only legitimate use for this project is *academic study*, it must now, repeat, be destroyed. Take your Tone Dialer to a golf course; balance it to the best of your ability on a standard, nonergonomic golf tee; grab a nine iron; and go for the hole-in-one. Or remove the naughty crystal from its secret hiding place and use your Tone Dialer for legitimate purposes only.

CHAPTER 5

FUN AND EASY: BUGS ALREADY IN PLACE

Perhaps you don't feel like building any surveillance equipment at the moment. Maybe you've had a bad experience with the wrong end of a soldering iron. Maybe you just plain don't feel like embarking on a major project just for the sake of spying on someone who probably doesn't deserve it. In any case, this chapter deals with the more convenient side of the surveillance industry: bugs that are already in place. Have fun!

TUNING INTO CORDLESS TELEPHONES

One of the most popular bugs today—for the old-fashioned spy and casual busybody alike—is the cordless telephone. It is important that you do not confuse a cordless telephone with a mobile phone or cellular phone. These will be discussed later. A cordless phone is actually a radio system consisting of a "base" unit that plugs into the wall, replacing your standard corded phone. The receiver, or "handset," sits atop the base, charging its batteries while not in use. When the user wishes to place or receive a call, the handset can be taken off the base, at which time it will operate the same as a regular phone, only the wires are replaced by radio signals. The user is then free to walk around, do chores, and perform other tasks while talking on the phone.

The beauty of the cordless telephone is that few people think of it as a bug. Even folks who know their cordless phone is actually a radio don't really believe that eavesdroppers are tuning in. This is because the average cordless phone users aren't quite sure how an eavesdropper could tune in. They also believe that the range of their cordless phone is much more limited than it really is. As they walk too far away from the base they start to lose the signal. They hear it "break up." This reinforces their fallacious idea that the cordless phone can only be picked up by their next-door neighbors, if at all.

Most cordless phone users are unaware that, in addition to the handset, the base is broadcasting. Not only does the base broadcast the conversation, it broadcasts both sides of the conversation—with significantly more output power than the handset. The handset is engineered for low power so that the rechargeable batteries hold their charge during long conversations. Because the base receives its power from the wall outlet, the engineers did not need to implement a low-power design. The average cordless phone users are completely ignorant of the fact that the real radio, the one they have to worry about, is the base, not the handset! The base thus acts as a latent, high-power radio transmitter, relatively speaking.

Combine all this with an eavesdropper's highly sensitive police scanner (the typical cordless handset is not all that sensitive) and you have a guy down the street making nachos entertaining himself with neighborhood gossip on a Saturday night.

Because most cordless phone users have a fundamental ignorance as to how the security of their communication can be breached, they tend to dismiss the unpleasant possibility altogether. A form of denial takes place even in

the face of widespread public advisories. The result is a very convenient and inexpensive surveillance mechanism or, for some people, an evening of cheap entertainment.

Yippee! How Do I Do It?

You need two pieces of equipment to monitor cordless phone conversations:

- A valid court-issued warrant
- A police scanner

The type of paper the warrant is printed on is not very crucial as long as it's signed by a judge. The type of scanner you use is more crucial. The scanner must be able to scan (or be programmed) in the 43-to-50 MHz band. The exact frequencies will be given later. A 100-channel programmable scanner works nicely.

The type of cordless phone best suited for scanner interception is any type that broadcasts an analog (voice) signal in what I affectionately refer to as "straight FM." Straight FM is a form of radio frequency modulation that can be received on an ordinary, unmodified FM receiver.

These types of cordless phones are produced by many manufacturers and operate in the 43-to-49 MHz radio frequency range. In no particular order, some such manufacturers are AT&T, Bell South, Motorola, Panasonic, Sony, and Uniden. If you noticed that, in fact, there was a particular order to the foregoing list then you are a pretty good detective and you deserve one "atta-person" (**NOTE**: "Atta-person" is the gender-neutral form of the now-defunct "attaboy." Eavesdropping has recently been declared a gender-neutral hobby by the High Saint of Political Androgyny.)

So, what are these frequencies anyway?

Well, the first cordless phones to hit the market in widespread popularity had base units that operated on 10 channels from 46.610 MHz to 46.970 MHz. The base unit is what we are mainly interested in because, as mentioned, it has greater output power and, more significant, broadcasts both sides of the conversation. The handsets accompanying these base units operate from 49.670 to 49.990. The frequencies for each channel are given in Table 1.

Table 1: 46/49 MHz Cordless Phone Frequencies

CH	BASE	HANDSET
1	46.610	49.670
2	46.630	49.770
3	46.670	49.830
4	46.710	49.845
5	46.730	49.860
6	46.770	49.875
7	46.830	49.890
8	46.870	49.930
9	46.930	49.970
10	46.970	49.990

Darkened cells indicate frequencies also used in baby monitors, low-power walkie-talkies, and remote-control models.

Program these frequencies into your scanner. If your scanner supports banks of 10 (such as 10 banks of 10 channels for a 100-channel programmable scanner), then all of the base frequencies will fit nicely into one bank. If you're curious about the handset frequencies, they will also fit nicely into one bank, but you only need the base frequencies to get both sides of the conversation.

Placing related frequencies into banks will prove more convenient as you learn more frequencies. It's helpful if all of your cordless phone frequencies are in bank-1 and all of your local police frequencies are in bank-2. When you want to listen to cordless, scan bank-1. If you want to see if the police are coming to ask you questions, scan bank-2. You get the idea.

Now, pop an antenna on your scanner and scan away. If you're in an urban apartment

complex, you should hear conversations on at least half of these channels from 4 P.M. to 8 P.M. when phone use is high. If you're in a rural location, you may not hear as many conversations. If you're very rural, you may need to drive around the neighborhood—but you WILL hear conversations! By the way, if you do plan to drive around with a handheld scanner, be aware that some local jurisdictions have ordinances against doing just that. I have my doubts as to whether such "laws," if challenged, will stand up in court, but just be aware of this.

New FCC Allocations: 44–48 MHz

The original FCC rules restricted cordless phone manufacturers to 10 frequencies in the 46-to-49-MHz range. In 1995, new FCC rules eliminated those restrictions, allowing for 15 new channels, and such manufacturers as AT&T, Uniden, and Bell South began manufacturing cordless phones with 25 channels instead of 10.

This next generation of straight FM analog cordless phones have base units broadcasting from 43.720 MHz to 44.480 MHz, in addition to the previously allocated frequencies. Since these frequencies are lower than the original allocations, the original 10 channels have been renumbered 16 to 25 and the new channels inserted as channels 1 through 15. The new phones function exactly the same as their predecessors, improvements in general technology excepted. For your enjoyment, Table 2 lists the new frequencies as taken from a BellSouth Model (HAC) 3901 cordless telephone.

Table 2: 44/46 MHz Cordless Phone Frequencies

CH	BASE	HANDSET
1	43.720	48.760
2	43.740	48.840
3	43.820	8.860
4	43.840	48.920
5	43.920	49.020
6	43.960	49.080
7	44.120	49.100
8	44.160	49.160
9	44.180	49.200
10	44.200	49.240
11	44.320	49.280
12	44.360	49.360
13	44.400	49.400
14	44.460	49.460
15	44.480	49.500
16	46.610	49.670
17	46.630	49.770
18	46.670	49.830
19	46.710	49.845
20	46.730	49.860
21	46.770	49.875
22	46.830	49.890
23	46.870	49.930
24	46.930	49.970
25	46.970	49.990

Darkened cells indicate frequencies also used in baby monitors, low-power walkie-talkies, and remote-control models.

Recognizing and Dealing with Voice Inversion

I'd like to mention a cordless phone security feature that you may come across from time to time. If you're scanning cordless phone frequencies and you hear something that sounds like severely distorted human voices, it's probably a security feature known as voice inversion. I believe Motorola makes a (rather expensive) voice-inversion 46–49 MHz cordless phone. The encoding scheme is not as sophisticated as others that we'll discuss later. Instead, it is a simple analog circuit that mangles the original voice signal into something unintelligible. Voice-inversion and

reversing circuits are available in kit form. You can find them from time to time in the back of electronics supplier catalogs. If you have Internet access, you may wish to search the archives of *rec.radio.scanner* or post an inquiry there. Occasionally, someone will post a good voice-reversing circuit in that newsgroup or others like it.

A company called CTP sells voice-inversion circuits in kit form or fully assembled. I highly recommend its DS49-CU1 stand-alone descrambler. I own one myself, and it works like a charm (on my home phone only, of course). CTP's address is as follows:

CTP
517 Lower Terrace
Huntington, WV 25705

You can also visit CTP's Web site at http://members.aol.com/ctpds49. Prices start at $39.95 for the inversion kit, and the company has lotsa other nifty items, many of which make great starter kits for the novice technician. It accepts Visa, MasterCard, Discover, and that other one there . . . American something.

Exposure Method

Another way to deal with voice-inversion scrambling is simply to listen to it regularly. Study the rise and fall in pitch of the scrambled voice. Study the pauses in conversation. Keep in mind that you already know the first few words of any conversation:

"Hello?"
"Hi."
"Hey! What's goin' on?"
"Not much. What about you?"
"Ahhh . . . nothin' really. Just sittin' around . . ."

Or words very similar. You get the idea. Also keep in mind that if things sound too foreign to you, it may be just that. You could be listening to a scrambled conversation in a foreign language. After a few minutes of this, you will need to unbend your brain. You will nonetheless notice the rise and fall of conversation remains the same no matter the language.

Hacking 900 MHz

Originally reserved for military use, the 900-MHz band is now available for commercial RF applications. The 900-MHz band allows for greater transmission distances and reduced static interference. Sound good? Well, not necessarily so for the would-be spy. With the advent of 900 MHz, manufacturers began implementing more sophisticated security features such as microprocessor-controlled voice scrambling and digital "spread-spectrum" technology. These signals are unintelligible on a standard FM receiver. Intercepting digital and spread-spectrum radio transmissions does not fall within the scope of "fun and easy" surveillance—we'll save that for another book. But there are a few analog 900-MHz cordless phones out there.

Some analog 900-MHz units are marketed to businesses as wireless headsets. The advantage is that you can work your secretary twice as hard; rendered wireless, your secretary can move about the office while fielding telephone calls. There are also some analog 900-MHz cordless phones marketed to the general public. Scanner reception for many of these models is difficult due to the frequency schemes used by the manufacturers. Most scanners scan the 900-MHz band in 12.5-KHz steps. Frequency allocations for 900-MHz cordless phones are often in 30-KHz steps. Thus, when scanning this frequency range, you are more likely to pick up cellular phone images rather than cordless.

There are, however, some very popular 900-MHz cordless phones still being sold today that are scanner friendly. Generally, any phone that has frequencies laid out in 50- or 100-KHz steps is scanner friendly. Here are a few frequency lists for your enjoyment; friendly phones are listed first.

Table 3: Panasonic KX-TCM939-B

CH	BASE	HANDSET
1	902.100	926.100
2	902.200	926.150
3	902.450	926.250
4	902.500	926.300
5	902.550	926.350
6	902.600	926.550
7	902.650	926.550
8	902.700	926.600
9	902.750	926.650
10	902.800	926.700
11	902.850	926.750
12	902.900	926.800
13	902.950	927.050
14	903.050	927.100
15	903.100	927.200
16	903.200	927.250
17	903.250	927.300
18	903.300	927.350
19	903.350	927.400
20	903.400	927.450
21	903.450	927.500
22	903.500	927.550
23	903.550	927.600
24	903.600	927.650
25	903.750	927.700
26	903.900	927.750
27	904.200	927.800
28	904.500	927.850
29	904.650	927.900
30	904.800	927.950

Table 4:
V-Tech Tropez DX900
20 Channels, 100-KHz Spacing
Base: 905.600 to 907.500
Handset: 925.500 to 927.400

CH	BASE	HANDSET
1	905.600	925.500
2	905.700	925.600
3	905.800	925.700
4	905.900	925.800
5	906.000	925.900
6	906.100	926.000
7	906.200	926.100
8	906.300	926.200
9	906.400	926.300
10	906.500	926.400
11	906.600	926.500
12	906.700	926.600
13	906.800	926.700
14	906.900	926.800
15	907.000	926.900
16	907.100	927.000
17	907.200	927.100
18	907.300	927.200
19	907.400	927.300
20	907.500	927.400

Table 5:
Panasonic KX-T9000
60 Channels, 30-KHz Spacing
Base: 902.100 to 903.870
Handset: 926.100 to 927.870

CH	BASE	HANDSET	CH	BASE	HANDSET
1	902.100	926.100	31	903.000	927.000
2	902.130	926.130	32	903.030	927.030
3	902.160	926.160	33	903.060	927.060
4	902.190	926.190	34	903.090	927.090
5	902.220	926.220	35	903.120	927.120
6	902.250	926.250	36	903.150	927.150
7	902.280	926.280	37	903.180	927.180
8	902.310	926.310	38	903.210	927.210
9	902.340	926.340	39	903.240	927.240
10	902.370	926.370	40	903.270	927.271
11	902.400	926.400	41	903.300	927.301
12	902.430	926.430	42	903.330	927.331
13	902.460	926.460	43	903.360	927.361
14	902.490	926.490	44	903.390	927.391
15	902.520	926.520	45	903.420	927.421
16	902.550	926.550	46	903.450	927.451
17	902.580	926.580	47	903.480	927.481
18	902.610	926.610	48	903.510	927.511
19	902.640	926.640	49	903.540	927.541
20	902.670	926.670	50	903.570	927.571
21	902.700	926.700	51	903.600	927.600
22	902.730	926.730	52	903.630	927.630
23	902.760	926.760	53	903.660	927.660
24	902.790	926.790	54	903.690	927.690
25	902.820	926.820	55	903.720	927.720
26	902.850	926.850	56	903.750	927.750
27	902.880	926.880	57	903.780	927.780
28	902.910	926.910	58	903.810	927.810
29	902.940	926.940	59	903.840	927.840
30	902.970	926.970	60	903.870	927.870

Digital

We have seen that analog signals intercepted on a standard FM receiver render intelligible audio for surveillance purposes, but you must also be aware that digital signals may be broadcast over the FM band. If you're scanning cordless phone frequencies and happen upon a signal that sounds hissy and inhuman, it is probably a digital signal. As with spread spectrum, we are not going to get into decoding digital signals in this book. That subject could be a book in itself.

The way it works is analog signals are digitally encoded before being broadcast. This increases the cordless phone's range two to three times the distance of analog. Unfortunately, this makes surveillance difficult because a scanner tuned into the digital conversation will only hear scrambled static.

Spread Spectrum

Spread-spectrum technology spreads a digital signal over several frequencies instead of locking onto just one. This technology continuously scans the airwaves looking for the clearest channels available and uses them. Spread-spectrum signals cannot be tracked with the methods we have studied.

Digitized Audio

Another form of voice encryption uses a microprocessor to scramble conversation 65,536 different ways. Decoding this type of transmission is beyond the scope of this chapter. Keep in mind, though, that if this technology sticks around for any length of time, I can guarantee that fone phreaks will find a way around it. One method already popping up on the Internet is to look for unscrambled analog audio leaking from the pre-amp circuits before digitization. For some models, it is rumored that such leakage does occur around 430 MHz. I have yet to hear this myself, and it is unclear how strong such "leakage signals" are. It's certainly worth looking out for, though.

Still Some Hope

Fortunately 900-MHz technology—scrambled, digital, digitized, spread spectrum, or plain vanilla—is still relatively expensive. Many businesses are converting to 900 MHz (and its associated technologies) as their equipment needs replacing. For the next several years, though, average Joe and Josephine will be monitored a million times over by people using the exact methods described above.

TUNING INTO CELLULAR TELEPHONES

A cell phone is a radio, right? So it can double as a friendly surveillance device as well, right? "Hey! Every book I ever read about monitoring cellular says that it's tricky and boring, and you can only hear bits and pieces of conversations! You're trying to trick me!"

Now, hold on there, partner. True, cellular cannot be monitored as easily as cordless, but with a little knowledge and imagination, it's not as difficult as everybody says.

The problem with monitoring cellular is that, without special knowledge, you will usually not know who you are monitoring. Compared to cordless technology, it's more difficult to target a specific conversation. For example, if your subject uses a cordless phone, you can simply pull up in front of her house, scan the relatively small number of cordless phone frequencies, and when she places or receives a phone call you'll be able to listen in on both sides of a nice, juicy conversation. This is not the case with cellular. A thorough understanding of cellular function, however, will make monitoring these wonderful surveillance devices a bit more pleasurable and considerably more productive.

The first hurdle in cellular monitoring is finding a scanner that will receive cellular frequencies. The Electronic Communications Privacy Act (ECPA) of 1986 made it illegal to monitor cellular telephone conversations without a warrant. Shortly thereafter, scanner manufacturers were forced to eliminate cellular frequencies from their scanners. It is now

impossible to buy a newly manufactured cellular-capable scanner in the United States of America. Remember to thank your congressional representative.

But cellular interception, my friends, is far from dead. If your scanner was manufactured before 1994, there's a good chance it can readily receive cellular—if not readily, then perhaps with some minor modification. Some scanners made after 1994 can also be modified for cellular interception. A good book on scanner modification is *The Ultimate Scanner* by Bill Cheek (available from Paladin Press).

Another alternative is to buy a cellular-capable scanner in a foreign market or find one in the used-scanner market. The point is that there are plenty of cellular-capable scanners out there. So if you plan to monitor cellular, go out and get a cellular-capable scanner (and, of course, a warrant from your happy local courthouse).

Understanding Cellular Systems

There are various cellular implementations in use throughout the world. By far the most popular in the United States is Advanced Mobile Phone Service (AMPS). Because it is still in wide use as this book is written, this is the system we will explore below. The reader should also be aware of a digital cellular implementation making its way into U.S. markets.

Personal Communication Service (PCS), also known to the Europeans as Global System Mobile (GSM) and to the Japanese as Personal Digital Cellular (PDC), is a digital cellular system implemented in the 1.8-to-1.9 GHz range. Other than the fact that I believe these frequencies will turn your brains into toast, its implementation is fundamentally the same as the AMPS system we'll be discussing. Because it is digital, however, voice signals cannot be readily picked up with a standard police scanner.

How Cellular Works

The term *cellular* simply means that the system of communication relies on cells. A cell is a geographical area serviced by a cell site. A cell site is a radio tower that a mobile unit (i.e., cell phone) can interface with. Call routing is controlled by a mobile telephone switching office (MTSO) servicing the cellular coverage area.

Typical phone calls break down in the following ways:

Residential to Mobile

A residential customer with standard (noncellular) phone service places a call to a mobile unit. The TelCo central office recognizes the exchange as a cellular subscriber and routes the call to the MTSO servicing the appropriate cellular coverage area. The MTSO determines the status of the cell phone. If it is busy, the MTSO returns a busy signal to the person originating the call. If the mobile unit is available, the MTSO broadcasts the mobile's phone number over the paging channel of each cell site in the service area. The mobile unit, upon recognizing its phone number, sends an acknowledgment to the MTSO via the same paging channel. The MTSO, via the cell site's control channel, then tunes the mobile unit to an available voice frequency (see Figure 31 beginning on page 77) from the nearest cell site. The MTSO causes the mobile unit to ring and sends an electronic ring signal back to the calling party. Once the call is connected, the MTSO monitors the mobile's signal strength in relation to all available cell sites. If mobile transmissions fall below a certain level, the MTSO will tune the mobile to a cell site receiving the strongest signal from the mobile.

Mobile to Residential

A call originating from a mobile breaks down the same, except in reverse. When the mobile goes "off hook" a page goes out requesting service. The MTSO determines the mobile's location and assigns it the strongest channel it can find. The MTSO then sets up the call and, if connected, performs the monitoring and cell site switching as described above.

Mobile to Mobile

These calls work the same except that there is no need to deal with a wireline service unless the call is to a different service area.

Frequency Breakdown

Each cellular service area is required by law to have at least two cellular service providers: a "wireline" service offered by the local telephone company and a nonwireline service offered by an independent company.

In 1974 the FCC allocated a 20-MHz bandwidth (from 870 to 890 MHz) for cellular base stations and a 20 MHz bandwidth (from 825 to 845 MHz) for cellular mobiles. These bandwidths were subdivided into 30-KHz steps. Each service provider, wireline and nonwireline, thus had 666 frequencies: 333 mobile and 333 base. Twenty-one of the base frequencies are used as control, setup, data, and paging channels.

The original allocations as broken down per service provider were as follows:

NONWIRELINE

Mobile: 825.030 MHz to 834.990 MHz
Base: 870.030 MHz to 879.990 MHz

WIRELINE

Mobile: 835.020 MHz to 844.980 MHz
Base: 880.020 MHz to 889.980 MHz

To accommodate growing market demand, the FCC has since granted each service provider an additional 5-MHz bandwidth. The entire 10 MHz bandwidth is broken down as follows:

Mobiles:
A 1-MHz bandwidth from 824 MHz to 825 MHz
A 4-MHz bandwidth from 845 MHz to 849 MHz

Bases:
A 1-MHz bandwidth from 869 MHz to 870 MHz
A 4-MHz bandwidth from 890 MHz to 894 MHz

Again broken down in 30-KHz steps, each service provider received 83 new frequencies. Here is the complete breakdown of all allocations to date:

NONWIRELINE

Mobiles:
824.040 to 834.990 MHz
845.010 to 846.480 MHz

Bases:
869.040 to 879.990 MHz
890.010 to 891.480 MHz

WIRELINE

Mobiles:
835.020 to 844.980 MHz
846.510 to 848.970 MHz

Bases:
880.020 to 889.980 MHz
891.510 to 893.970 MHz

An additional 4-MHz bandwidth has been set aside by the FCC. These are a 2-MHz bandwidth from 849 to 851 MHz and a 2-MHz bandwidth from 894 to 896 MHz. I'm assuming that these are reserved for future cellular expansion as needed.

"Great! Now I can run out and monitor cellular!" Well, sort of. You can scan these frequencies and pick up bits and pieces of conversations, but you will have no idea who you are listening to. Nor will you have any way of targeting a particular subject. It will be boring—just as everybody has been saying.

There's still more to learn, but go ahead—get that warrant and scan away. Get it out of your system. I'll wait.

Handoffs and Flea-Flickers

Okay, so you've scanned some cellular frequencies, and you're beginning to get the idea. The conversations are spotty, to say the least. The thing that's going to make you a cellular-scanning maven is knowing how to arrange and organize cellular frequencies into

your scanner to track conversations as the mobile moves through different cells.

If you tried scanning some of the base frequencies, you noticed one annoying fact about cell site monitoring: many of the conversations seem to end abruptly. Well, the conversations are not really ending. What's happening is that the MTSO, upon sensing that the mobile is going out of range of the current cell site, decides to "hand off" the conversation to another frequency, usually in another cell. (It may help you to reread the section on how cellular works. It's vital that you understand this.)

Here is an analogy: think of a cellular telephone conversation as a football and a cell site as a running back. The running back carries the ball as far as he can until he encounters interference (e.g., signal loss). The running back then looks around for another running back who is in a better position to carry the ball. The running back in possession of the ball then hands off, or laterally passes the conversation, oops, I mean football to the other running back who is in the clear. If cells didn't hand off to one another, the conversation would simply die when the user drives out of range.

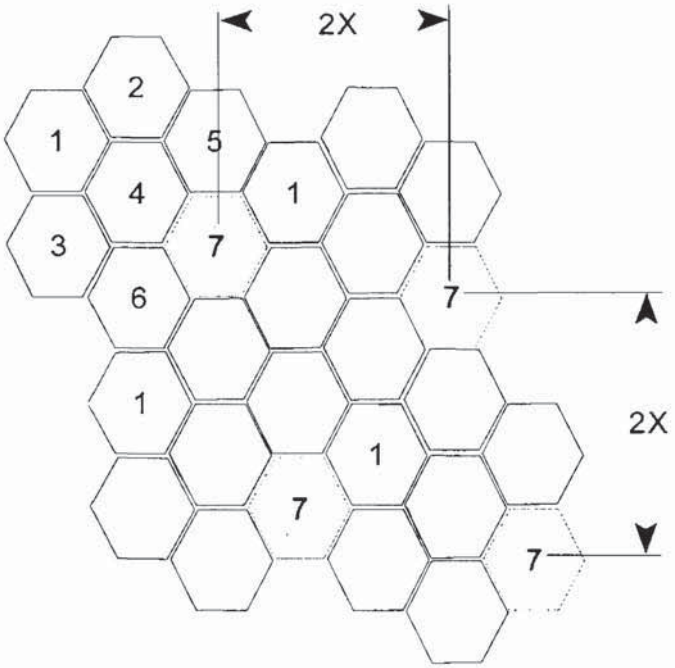


Figure 30. Typical cell block arrangement for seven-cell layout.

The Cell Site

Figure 30 shows a cellular service area broken down into individual cells represented by hexagons. In a typical cellular coverage area, these cells are arranged in groups of seven. Each group of seven is called a cell block. The reason for this arrangement is due to the limited number of frequencies that the cellular service provider has at its disposal. Because of their limited numbers, these frequencies will have to be reused even in areas of low-to-moderate population density. By arranging cells in a certain manner, cellular service providers can ensure that cells using the same frequencies are separated by a minimum distance. Without this separation, the reused frequencies would interfere with each other, causing serious engineering headaches for the cellular service provider.

Because phone companies like to make money, it is important to them that each cell site be able to service more than one call at a time. Thus, each cell site has many frequency channels for its subscribers to use. So which frequencies are in which cells? That's the $65,536 question, isn't it? The truth is that cellular implementation can vary from area to area. The frequency distribution scheme that accompanies the typical cell block arrangement is shown in Figure 31.

Upon studying the distribution scheme in Figure 31, you will notice that there are actually 21 groups of frequencies for each service provider (wireline and nonwireline). You will also note that rather than being labeled consecutively from 1 through 21, they are labeled 1A to 7A, 1B to 7B, and 1C to 7C. This is because cellular implementation is designed using directional antennae.

NON-WIRELINE BASE FREQUENCY DISTRIBUTION PLAN						
1A	2A	3A	4A	5A	6A	7A
870.030	870.060	870.090	870.120	870.150	870.180	870.210
870.660	870.690	870.720	870.750	870.780	870.810	870.840
871.290	871.320	871.350	871.380	871.410	871.440	871.470
871.920	871.950	871.980	872.010	872.040	872.070	872.100
872.550	872.580	872.610	872.640	872.670	872.700	872.730
873.180	873.210	873.240	873.270	873.300	873.330	873.360
873.810	873.840	873.870	873.900	873.930	873.960	873.990
874.440	874.470	874.500	874.530	874.560	874.590	874.620
875.070	875.100	875.130	875.160	875.190	875.220	875.250
875.700	875.730	875.760	875.790	875.820	875.850	875.880
876.330	876.360	876.390	876.420	876.450	876.480	876.510
876.960	876.990	877.020	877.050	877.080	877.110	877.140
877.590	877.620	877.650	877.680	877.710	877.740	877.770
878.220	878.250	878.280	878.310	878.340	878.370	878.400
878.850	878.880	878.910	878.940	878.970	879.000	879.030
879.390	**879.420**	**879.450**	**879.480**	**879.510**	**879.540**	**879.570**
890.010	890.040	890.070	890.100	890.130	890.160	890.190
890.640	890.670	890.700	890.730	890.760	890.790	890.820
891.270	891.300	891.330	891.360	891.390	891.420	891.450
869.400	869.430	869.460	869.490	869.520	869.550	869.580

WIRELINE BASE FREQUENCY DISTRIBUTION PLAN						
1A	2A	3A	4A	5A	6A	7A
880.020	**880.050**	**880.080**	**880.110**	**880.140**	**880.170**	**880.200**
880.650	880.680	880.710	880.740	880.770	880.800	880.830
881.280	881.310	881.340	881.370	881.400	881.430	881.460
881.910	881.940	881.970	882.000	882.030	882.060	882.090
882.540	882.570	882.600	882.630	882.660	882.690	882.720
883.170	883.200	883.230	883.260	883.290	883.320	883.350
883.800	883.830	883.860	883.890	883.920	883.950	883.980
884.430	884.460	884.490	884.520	884.550	884.580	884.610
885.060	885.090	885.120	885.150	885.180	885.210	885.240
885.690	885.720	885.750	885.780	885.810	885.840	885.870
886.320	886.350	886.380	886.410	886.440	886.470	886.500
886.950	886.980	887.010	887.040	887.070	887.100	887.130
887.580	887.610	887.640	887.670	887.700	887.730	887.760
888.210	888.240	888.270	888.300	888.330	888.360	888.390
888.840	888.870	888.900	888.930	888.960	888.990	889.020
889.470	889.500	889.530	889.560	889.590	889.620	889.650
891.600	891.630	891.660	891.690	891.720	891.750	891.780
892.230	892.260	892.290	892.320	892.350	892.380	892.410
892.860	892.890	892.920	892.950	892.980	893.010	893.040
893.490	893.520	893.550	893.580	893.610	893.640	893.670

Figure 31. Frequency distribution scheme for wireline and nonwireline cell companies.

NON-WIRELINE BASE FREQUENCY DISTRIBUTION PLAN						
1B	2B	3B	4B	5B	6B	7B
870.240	870.270	870.300	870.330	870.360	870.390	870.420
870.870	870.900	870.930	870.960	870.990	871.020	871.050
871.500	871.530	871.560	871.590	871.620	871.650	871.680
872.130	872.160	872.190	872.220	872.250	872.280	872.310
872.760	872.790	872.820	872.850	872.880	872.910	872.940
873.390	873.420	873.450	873.480	873.510	873.540	873.570
874.020	874.050	874.080	874.110	874.140	874.170	874.200
874.650	874.680	874.710	874.740	874.770	874.800	874.830
875.280	875.310	875.340	875.370	875.400	875.430	875.460
875.910	875.940	875.970	876.000	876.030	876.060	876.090
876.540	876.570	876.600	876.630	876.660	876.690	876.720
877.170	877.200	877.230	877.260	877.290	877.320	877.350
877.800	877.830	877.860	877.890	877.920	877.950	877.980
878.430	878.460	878.490	878.520	878.550	878.580	878.610
879.060	879.090	879.120	879.150	879.180	879.210	879.240
879.600	**879.630**	**879.660**	**879.690**	**879.720**	**879.750**	**879.780**
890.220	890.250	890.280	890.310	890.340	890.370	890.400
890.850	890.880	890.910	890.940	890.970	891.000	891.030
891.480	X	869.040	869.070	869.100	869.130	869.160
869.610	869.640	869.670	869.700	869.730	869.760	869.790

WIRELINE BASE FREQUENCY DISTRIBUTION PLAN						
1B	2B	3B	4B	5B	6B	7B
880.230	**880.260**	**880.290**	**880.320**	**880.350**	**880.380**	**880.410**
880.860	880.890	880.920	880.950	880.980	881.010	881.040
881.490	881.520	881.550	881.580	881.610	881.640	881.670
882.120	882.150	882.180	882.210	882.240	882.270	882.300
882.750	882.780	882.810	882.840	882.870	882.900	882.930
883.380	883.410	883.440	883.470	883.500	883.530	883.560
884.010	884.040	884.070	884.100	884.130	884.160	884.190
884.640	884.670	884.700	884.730	884.760	884.790	884.820
885.270	885.300	885.330	885.360	885.390	885.420	885.450
885.900	885.930	885.960	885.990	886.020	886.050	886.080
886.530	886.560	886.590	886.620	886.650	886.680	886.710
887.160	887.190	887.220	887.250	887.280	887.310	887.340
887.790	887.820	887.850	887.880	887.910	887.940	887.970
888.420	888.450	888.480	888.510	888.540	888.570	888.600
889.050	889.080	889.110	889.140	889.170	889.200	889.230
889.680	889.710	889.740	889.770	889.800	889.830	889.860
891.810	891.840	891.870	891.900	891.930	891.960	891.990
892.440	892.470	892.500	892.530	892.560	892.590	892.620
893.070	893.100	893.130	893.160	893.190	893.220	893.250
893.700	893.730	893.760	893.790	893.820	893.850	893.880

NON-WIRELINE BASE FREQUENCY DISTRIBUTION PLAN

1C	2C	3C	4C	5C	6C	7C
870.450	870.480	870.510	870.540	870.570	870.600	870.630
871.080	871.110	871.140	871.170	871.200	871.230	871.260
871.710	871.740	871.770	871.800	871.830	871.860	871.890
872.340	872.370	872.400	872.430	872.460	872.490	872.520
872.970	873.000	873.030	873.060	873.090	873.120	873.150
873.600	873.630	873.660	873.690	873.720	873.750	873.780
874.230	874.260	874.290	874.320	874.350	874.380	874.410
874.860	874.890	874.920	874.950	874.980	875.010	875.040
875.490	875.520	875.550	875.580	875.610	875.640	875.670
876.120	876.150	876.180	876.210	876.240	876.270	876.300
876.750	876.780	876.810	876.840	876.870	876.900	876.930
877.380	877.410	877.440	877.470	877.500	877.530	877.560
878.010	878.040	878.070	878.100	878.130	878.160	878.190
878.640	878.670	878.700	878.730	878.760	878.790	878.820
879.270	879.300	879.330	879.360	X	X	X
879.810	**879.840**	**879.870**	**879.900**	**879.930**	**879.960**	**879.990**
890.430	890.460	890.490	890.520	890.550	890.580	890.610
891.060	891.090	891.120	891.150	891.180	891.210	891.240
869.190	869.220	869.250	869.280	869.310	869.340	869.370
869.820	869.850	869.880	869.910	869.940	869.970	870.000

WIRELINE BASE FREQUENCY DISTRIBUTION PLAN

1C	2C	3C	4C	5C	6C	7C
880.440	**880.470**	**880.500**	**880.530**	**880.560**	**880.590**	**880.620**
881.070	881.100	881.130	881.160	881.190	881.220	881.250
881.700	881.730	881.760	881.790	881.820	881.850	881.880
882.330	882.360	882.390	882.420	882.450	882.480	882.510
882.960	882.990	883.020	883.050	883.080	883.110	883.140
883.590	883.620	883.650	883.680	883.710	883.740	883.770
884.220	884.250	884.280	884.310	884.340	884.370	884.400
884.850	884.880	884.910	884.940	884.970	885.000	885.030
885.480	885.510	885.540	885.570	885.600	885.630	885.660
886.110	886.140	886.170	886.200	886.230	886.260	886.290
886.740	886.770	886.800	886.830	886.860	886.890	886.920
887.370	887.400	887.430	887.460	887.490	887.520	887.550
888.000	888.030	888.060	888.090	888.120	888.150	888.180
888.630	888.660	888.690	888.720	888.750	888.780	888.810
889.260	889.290	889.320	889.350	889.380	889.410	889.440
889.890	889.920	889.950	889.980	890.010	890.040	890.070
892.020	892.050	892.080	892.110	892.140	892.170	892.200
892.650	892.680	892.710	892.740	892.770	892.800	892.830
893.280	893.310	893.340	893.370	893.400	893.430	893.460
893.910	893.940	893.970				

Refer to Figure 32. Ideally, the cell site (antenna tower and associated hardware) is placed at the center of a cell. In this diagram the actual cell is represented by a dotted line. The arrows show the directionality of the antennae and the solid hexagons depict a different way of envisioning a cell. In the case of the solid hexagon scheme, antenna placement is in the three opposite corners of the hexagon, marked by the lowercase letters.

I've seen many theories floating around in scanner newsgroups and related publications about cellular implementation and whether cells are arranged in blocks of 7 or 21. Hopefully, the foregoing description will help clear that up. Do keep in mind, however, that actual cellular implementation will vary from coverage area to coverage area. Using these charts and knowing the concepts involved is a nice starting point for mapping your own cellular coverage area (or that of your subject).

How Does All This Help?

"Gee, Mr. Charrett, you sure did give me a lot of information on cellular implementation, but how does all this help me monitor cellular phone conversations after I get my court-issued warrant? And how do I know when my subject is using his cell phone?"

Well, those are some damn fine questions, and they deserve some damn fine answers. First, let me state that this information will be a hundred times more useful to you if you know when your subject is on his cell phone. This is the job of the detective, though. There are a zillion different scenarios, and I'd be foolish to attempt to cover them here. Just do good detective work and you'll figure out your subject's habits—cell phone use and all.

Second, let me say that this information will be a thousand times more useful to you if you've mapped the cellular implementation of the target area (where your subject lives, works, or generally likes to talk on the cell phone). Mapping a cellular coverage area is discussed in the next section. Even if you don't map the target area, the above information will still come in handy for tracking cellular conversations.

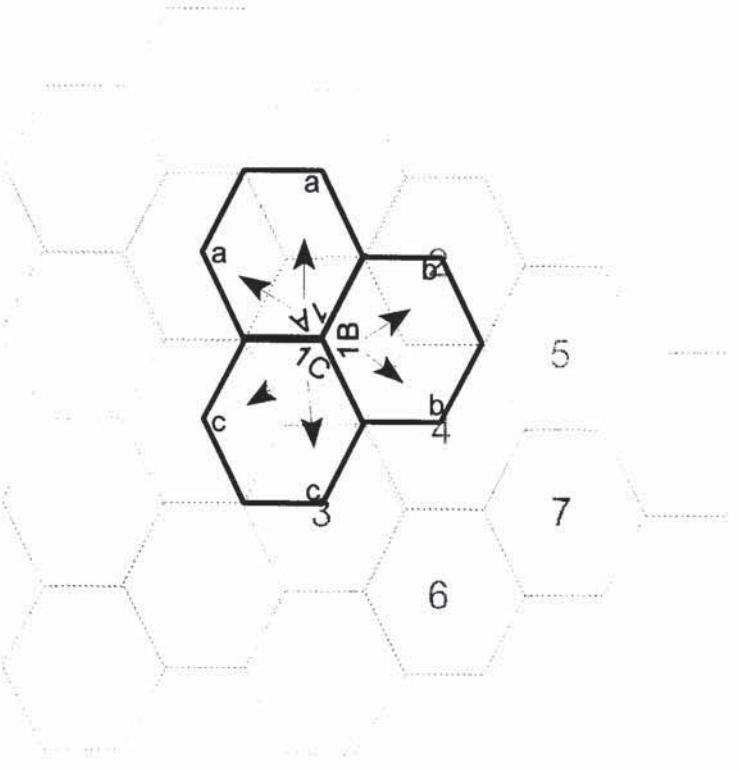


Figure 32. Antenna placement can be thought of in two ways. The antenna tower can be thought of as being at the cell center radiating waves in three directions, as represented by the dotted hexagons, or you can think of it as three separate antenna towers placed at the cells' opposite corners. The lowercase letters represent the opposite-corner towers in the solid hexagons.

Just knowing the conversation has been handed off is a great help in itself. Once your target conversation has been handed off, you can limit-search the cellular frequency allocations and attempt to find the conversation on its new channel. Knowing that wireline service providers use different frequencies than nonwireline providers is also a great help. If your subject subscribes to a nonwireline service, you only need to search through nonwireline frequencies. This cuts your search time in half.

Limit-searching through all available cell frequencies, though, is time consuming, even if your job is cut in half by knowing your subject's service provider. Chances are, your subject will have terminated the call before you find the handoff frequency. But if you have the cellular frequencies preprogrammed into your scanner, broken down so that each scanner bank holds all the frequencies to one cell (1A, 1B, and 1C), your job gets much easier. When your subject's conversation gets handed off to another frequency, you only need to scan the frequencies of adjacent cells (in most cases) to find the new conversation. This saves the operative considerable time and aggravation.

Now, before we go any further, a couple of things need explaining. You may have already noticed that to program a scanner to mimic the frequency distribution of a cellular coverage area, you will need a scanner that can support 60 channels in each of seven banks or 20 channels in each of 21 banks. You will find that the memory configuration of most cellular-capable scanners will not support either of these configurations. There are four alternatives:

- Modify a cellular-capable scanner for expanded memory.
- Use a 400-channel scanner to accommodate 395 voice frequencies.
- Use more than one scanner.
- Use the "poor man's cell hacking" method described below.

Scanner Modification

This subject is well covered in *The Ultimate Scanner* by Bill Cheek, who has written extensively on this subject (see the Bibliography). In his book(s), pay particular attention to his memory modification suggestions for the PRO-2004/5/6 series because many of these models are cellular-capable. The revisions that are not cellular capable may, in most cases, be modified to receive cellular.

Use a 400-Channel Scanner

Again, your best bet is the PRO-2005/6 or a modified PRO-2004. The PRO-2004 is probably better, but you will need to add a 1N4148 diode to the empty spot at D-510 to upgrade it from 300 to 400 channels. While you're in there you might as well add a 1N4148 diode at the empty spot for D-514, which provides a 25-percent speedup of the SCAN mode without compromising any other aspect of the scanner's functionality. These common modifications are well covered in various newsgroups and related literature, but I still recommend Mr. Cheek's book if you plan on doing any serious scanner hacking.

There are currently 416 available voice frequencies (per service provider), but 21 of them are being used for control channels. Doing the math, you have 395 voice frequencies, which will fit into a 400-channel scanner. One note on control frequencies: I, or rather a passing acquaintance of mine, found that control channels sometimes double as voice channels and vice versa. So before you make any assumptions about which 21 channels to leave out of your scanner banks, do some research!

Use Several Scanners

If you can obtain several cellular-capable scanners with 80-, 100-, or 200-channel programmable memory (such as earlier PRO-46 models), you can use one scanner per cell site. If you've thoroughly mapped your target area, there is actually an advantage to doing this. For example, if you have seven scanners, you can use an 800-MHz directional antenna

on each one. Each scanner can service one cell site (be sure to remember to point your antennae to their respective cell sites).

Sometimes your subject will give you a clue as to his location and direction of travel. Usually these clues come at the beginning of the conversation.

"Ring, ring."

"Hello?"

"Hey, it's Jake."

"You sound horrible."

"Yeah, I'm on my car phone."

"Where are you?"

"I'm on the turnpike by the Howard Johnson's."

"Oh yeah? What're ya doin' there?"

"Headin' up to the mall. Listen, I got somethin' . . . "

If you're at all familiar with the target area, this much information should give you the subject's location and direction of travel. When the MTSO hands off the conversation to the next cell site, you should have a pretty good guess about which cell site the subject is heading toward. Turn up the volume on the scanner covering that cell site and keep hitting the scan button until you reencounter the conversation. On cell borders, sometimes the conversation will be handed back to the previous cell. If so, just turn up the volume of the first scanner again and tune in!

Poor Man's Method

If you've only one 100-channel programmable scanner, here is a good trick to get you started. This example assumes your subject subscribes to a nonwireline service, but the method can be used to track wireline calls as well (just insert the appropriate frequencies). Follow these steps:

Procedure

1. Get a court-issued warrant and tell a judge he'd better sign it right now, damn it, or else!
2. Find the cell nearest you (or your subject) and program your scanner with the appropriate frequencies. There will be about 60 frequencies, which will fit into six banks. You will have four banks of 10 left over for local police and cordless phones.
3. Program your "limit-search" mode to cover 890.010 to 891.480 MHz (891.510 to 893.970 MHz for wireline).
4. Find a conversation you are interested in tracking. For our example, let's say the conversation is taking place on 870.030 MHz.
5. Press the MANUAL button on your scanner to monitor that channel.
6. When the conversation is handed off, press the DOWN search arrow. The scanner will stop at the next frequency carrying a conversation. If this happens to be your subject's conversation, continue listening and consider yourself the luckiest human in existence. Otherwise, keep hitting the DOWN arrow until you find your subject or until your display reads 869.040 MHz or less.
7. At this point, you are outside the cellular band. Hit the UP search arrow. Again, the scanner will stop at the next frequency containing a conversation (you will have heard some of these conversations on your way down the frequency spectrum). If the scanner stops on your subject's conversation—great!—continue listening. Otherwise, hit the UP search arrow. Keep doing this until you find your subject or until your display reads 879.990 MHz or higher.
8. At this point, you are outside the nonwireline cellular band.
9. Hit PROGRAM, LIMIT, then the UP or DOWN arrow to start searching the rest of the nonwireline band (the most recent FCC allocations). You set this up in step 3.
10. Most of the time you will have found your subject before this procedure is completed. If not, you will need to start over. To do this . . .
11. Press SCAN and scan the six banks holding the frequencies to your local cell. Keep pressing scan to see whether your subject is back in the local cell. After you have cycled through all six banks without finding your

subject, hit MANUAL and then begin again at step 7 as if the conversation had just been handed off.

12. This will often get you back to your subject. Keep in mind, however, that the longer it takes you, the less chance you have of reencountering the conversation.

Take Your Pick

There are several variations of the above handoff-tracking routine. The exact method you use will depend on your budget and what kind of equipment you have access to. Regardless of the exact method, handoff tracking works surprisingly well, especially if you've mapped your cell area. Once you get the hang of it, you will be pleasantly surprised at how little of any given conversation is lost to search time.

Unless you're going to bite the bullet and map your cellular coverage area, the poor man's method is probably the best technique to use. The other three methods best show off their utility and power when used in a mapped cell area. Although the above cell block layouts and frequency distribution schemes may be helpful as a general guide, you should be forewarned that cellular service engineers implement certain diversity schemes to compensate for predicted path loss, signal fading, and other less predictable radio propagation phenomena. Among the factors considered by the engineers are the following:

- Antenna directionality, height, and polarization
- Texture of the terrain, hills, buildings, and other obstructions
- Population density, expected growth, and future market demand
- Signal strength, harmonic intermodulation, and interference from other radio towers, including their own

The calculations involved in working with all these factors (and more) rival those of quantum mechanical models describing the beginning of the universe. You can therefore bet that actual cellular implementation will vary from area to area and bear only a minimal resemblance to the neat, looks-good-on-paper models depicted above. That said . . .

Mapping a Cellular Coverage Area

Mapping a cellular coverage area means that you take steps toward determining the locations and frequency distribution schemes of cell sites in any given target area. There are several different ways to accomplish this—none of them easy.

If you're God, or if you have a friend who works for the local cellular service provider, you may be able to get hold of some cell maps directly.

Or you can tell the FCC that you're doing feasibility research for a company thinking about starting a nonwireline cellular service and you believe you have the right to certain information in its files. Don't hold your breath.

You could also go to a holistic medical practitioner, get diagnosed with "electromagnetic poisoning" and file a lawsuit against the local cellular service provider. During the discovery period, you can then send the provider interrogatories relative to its antenna sites, frequency use, power output, etc. This, of course, will draw a lot of attention to you.

But if you'd really like to learn something and have fun doing it, you can map the cell area yourself, which, though still a monumental task, will probably take less time than any of the above methods.

The cell-mapping approach discussed below employs three, low-budget techniques. Although it is possible to make a cell map by using each technique individually, the do-it-yourself cellular cartographer will surely find that these methods, when used in conjunction with each other, will render a more thorough finished product in less time than if used separately. The methods we will discuss are these:

- Measuring relative signal strength
- Spying on yourself
- Visually locating and identifying cell sites

You will notice that the first method involves making measurements. So go out right now and spend $30,000 on a top-of-the-line frequency counter, SWR meter, and S-meter. Just kidding! Hey, if you've got the $30K to blow, then by all means, blow it. But if you don't . . .

Measuring Relative Signal Strength (The Poor Man's Approach)

For simplicity, we will assume that you are mapping a nonwireline cellular coverage area. As always, these methods can be adapted for wireline providers as well. Just remember to change the frequencies. The following procedure involves collecting information and charting it. (See Figure 33 for a blank chart and use notes. You may make copies of the blank chart for your own use. Refer to Figure 34 to see how the chart is used.)

Procedure

1. Wait for Congress to pass a law declaring cell mapping a legal pastime. Or get a warrant.
2. Wait for peak cell phone use hours (usually around rush hour).
3. Take the antenna off your scanner. (This is not a misprint!)
4. Turn the squelch all the way up.
5. Limit-search between 869.040 and 879.990.
6. Make sure the DELAY feature of your scanner is set to "ON" or "DLY."
7. Do this until your scanner stops at a "live" cell site (one on which there is a conversation).
8. Write down the frequency and associated vital signs in your chart. (See Figures 33 and 34 for chart and use notes.)
9. Keep doing this. Try to find as many frequencies as you can and write them down.
10. Turn your squelch down as low as it can go without causing the scanner to lock onto empty channels. We'll call this "edge mode."
11. Repeat steps 4 through 9.
12. Make a 1-inch antenna out of a fat paper clip and put it on your scanner.
13. Repeat steps 4 through 9.
14. Make a 2-inch antenna out of a fat paper clip and put it on your scanner.
15. Repeat steps 4 through 9.
16. Make a 4-inch antenna out of a fat paper clip and put it on your scanner.
17. Repeat steps 4 through 9.

No, I haven't gone mad. By using this method, we begin to get a picture of which cellular frequencies are strongest. For example, a strong signal received with the squelch all the way up and no antenna is stronger than a weak signal that can only be received with the squelch on "edge" and a 1-inch antenna. I do not recommend using a whip antenna, even if it is fully collapsed. The RF circuitry in scanners is very sensitive, and you will pull in too many cell sites to make an effective study.

By making a comparative study of the strongest frequencies, we begin to get an idea of the frequency distribution scheme used by the cellular engineers. Find all of your strongest frequencies and highlight them in Figure 31. Notice a pattern? More often than not, most of the strongest signals will be located in one column. For our example, let's say this pattern is in column 1A. This is because your listening post is located in cell number 1 and the "A" antennae are pointing toward you. Depending on your location, the second-strongest signals will be coming from another antenna in the same cell (1B or 1C) or the antenna of an adjacent cell that is also pointing at you (such as 2C or 7B). Please note that the individual cells will not necessarily follow the neat seven-cell layout of a typical cell block as shown in Figure 30. Along desolate highways, for example, it would not be unusual to see the same two or three cells reused in an alternating pattern. The actual cellular layout is what you are trying to map.

Using Figure 33, make your own computer database with Microsoft Works or other database software with which you are familiar. Keep all your entries on disk and when you have built up enough information, you can use a record-sorting routine (available in all

	Cell	FREQ	Area Covered	ANT	SQL	SIG	HO FREQ
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							

Figure 33. Use this chart to map your target cell area. You may make copies for that purpose if you wish.

	Cell	FREQ	Area Covered	ANT	SQL	SIG	HO FREQ
1	1A	870.660	"South Street @ the lights"	0"	FUL	S+	879.300
2	2C	879.300	"Getting on the on-ramp"	0"	EDG	S	END
3							
4	1C	869.190	"In the Best Western parking lot"	1"	EDG	M	875.700
5	1A	875.700	"South Street, stopped in traffic"	0"	FUL	S	878.040
6	2C	878.040	"Man this highway traffic sucks"	0"	EDG	M+	END

Figure 34. This sample chart shows you how the blank cell-mapping chart is intended to be used.

modern database software) to sort your records by signal strength, antenna length, measurement area, etc. By doing this you can more quickly get an overall picture of cellular implementation of your target area. A Microsoft Works (WDB) version of this database is available from my Web site (see Appendix D).

To better understand how to use the chart in Figure 33, look at the sample entries in Figure 34. The information in the first two entries was taken while tracking a certain cell phone conversation using any of the handoff tracking routines previously discussed. The next three entries were also taken during a single conversation. It's helpful to leave a blank space between conversations.

Entry 1 shows that the mapper's scanner stopped at 870.660, at which point he heard a conversation worth tracking. Immediately, the mapper entered in the vital information pertaining to antenna length (ANT), squelch position (SQL), and signal strength (SIG). Then, he looked up the frequency in Figure 31, found that it belongs to cell 1A, and entered this information under the cell column (Cell).

Early in the conversation, the owner of the mobile unit said, "I'm on South Street at the lights." Since this information is valuable to the cellular cartographer, he entered it in the "Area Covered" column. Shortly after that, the MTSO handed off the conversation. The mapper immediately began scanning until he reencountered the conversation on 879.300 MHz. He wrote this in as the handoff frequency (HO FREQ).

He also used this frequency as the starting point for entry 2 and filled in all of the vital information as it became available. When the MTSO handed off the signal again, he was unable to reencounter it. He noted this by entering the word "END" in the handoff column.

This particular cellular cartographer was having a lucky day. The next conversation he tracked gave the information in entries 4, 5, and 6. Much of this information seemed to corroborate theories he had already formed based on the previous entries.

Here's the theory:

> Since 1A gives the strongest signal, the "1" cell is probably closest, and the "A" antenna is probably pointing in the direction of the mapper. Cell 1A seems to have borders at the highway on-ramp and the traffic light area of South Street. Cell 1C does not give a very good signal; therefore, the "C" antenna of cell "1" must be pointing away from the mapper. Cell 2C seems to cover the local section of highway. Can you see why the cell mapper formed these theories? In time, you will be able to see these connections with ease. For now, let's explore another cell-mapping method to complement what you've already learned.

Spying on Yourself

An often-overlooked approach to cell mapping is the simple process of spying on yourself. Here's the procedure:

Procedure

1. Subscribe to a cellular service provider and ask for the "free nights and weekends" plan.
2. During your "free" time, and as close to rush hour as possible, call a local cinema that has 14 movies playing.
3. When the cinema's recording starts, put the cell phone down.
4. Scan the appropriate cell frequencies (wireline or nonwireline depending on your service) until you find your call (you'll hear the movie announcer bellowing gaily, " . . . and in cinema three this evening, *Blood & Guts* playing at 4:50, 7:15, and 9:45; in cinema four, *Sax & Violins*, playing at . . .").
5. To make sure it's your call and not some other moviegoer, tap the cell phone a few times and listen for the tapping over your scanner (or talk into it or put it in a blender or whatever).
6. Write down the frequency.
7. Repeat steps 1 through 6 several times.[1]
8. Compare your information with Figure 31.
9. Go to another location[2] and repeat steps 1 through 8.
10. If you want more information, repeat step 9.

The "Spying on Yourself" method will work even if you don't place a call (though it's not quite as fun as keeping the movie line tied up). This may be useful if you do not subscribe to a plan that offers "free" airtime. Sit by your home telephone with a cell phone and a sandwich (sandwich is optional). Make sure your home answering machine is off and dial your home number. Just let the phone ring. Scan the cell frequencies with your left hand and rub the cell phone on your pant leg with your right hand (or bang it against your head, scratch it, kick it or whatever—just make some noise). Your scanner will eventually lock onto a frequency broadcasting a background ring and a rubbing, banging, kicking, scratching, or blending sound.

What's the Point?

The point is that you're letting the cellular switching equipment do all your work for you! Think about it: if you make a cell call from a certain area and the MTSO assigns you a certain frequency (found with your handy-dandy scanner), then that frequency will normally be a frequency resident in the cell closest to your current location. Each time you call, you will usually receive a different frequency. To better ensure that you will be assigned a different frequency with each call, it is best to employ this procedure while cell phone use is moderately high. Otherwise, it's possible you will keep getting the same one or two frequencies. If cell phone use it too high, you run the risk of getting handed off to an adjacent cell because your local cell is full. This will give you false readings and therefore must be avoided.

You really don't need to call 60 times unless you're the thorough type, or unless your target area does not seem to follow a 630-KHz frequency separation plan. Once you've compared your results with Figure 31 and figured out what cell site is closest to you, you can move on to a new location and start again.

By repeating this method at various locations, you can map any cellular service area, anywhere at any time. If you do some careful planning, you will bring a map of the

1. You will hopefully be assigned a different frequency each time. To get all the frequencies in a given cell, you have to do this up to 60 times. Since you are at a fixed location, however, you will likely only be assigned to any of the 20 or 21 frequencies "pointing" at you via directional antennae. If you're on the cusp of two directional antennae or at a cell edge, the MTSO may assign you frequencies on either antenna or cell site. If you happen to be smack dab in the middle of three cell site antennae (such as 1A, 1B, and 2C) your measurements may be even more convoluted. By combining the "Spying on Yourself" procedure with the visual inspection procedure, you will gather more reliable data and greatly improve overall results.

2. The other location can be anywhere from a few hundred feet to 6 miles (or more) away from your present location. The reasons for this are explained in the upcoming section, "Visually Locate and Identify Cell Sites."

area with you. Every time you're sure you've discovered which cell site is serving a particular area write down the corresponding cell site number from Figure 31 (1A, 2B, 7C, etc.) on your map. Try not to "guestimate" your location; be as accurate as possible. This will save you major headaches as your map nears completion.

Visually Locate and Identify Cell Sites

Cell sites are typically found along major roadways on top of hills and buildings. When you find one of these, note its location on your cell map.

You may find many cell sites in the heart of a big city. As you drive away from the city, you will find fewer cell sites. This is because cells in cities are closer together than cells in more rural locations. By maintaining the ability to vary cell size, cellular engineers can accommodate market demand as it grows. If there were an unlimited number of legal frequencies, the cellular service providers could just add frequencies to existing cell sites as their demand grows. But the FCC has only allocated a limited number of frequencies. The cellular service providers have only one option to accommodate growing market demand: make more cells. To prevent interference from frequency reuse, cells placed close together (in the city center) must have less broadcast power than suburban cells.

To give you an idea of range, it is not unusual for a city cell to be dedicated to a radius of only a few hundred feet. On the other hand, it is not unusual for a suburban cell to cover a 6-mile radius. You may wish to keep these facts in mind when mapping your target area. Figure 35 shows how cell sizes shrink as population density increases.

Once you've gathered sufficient data to

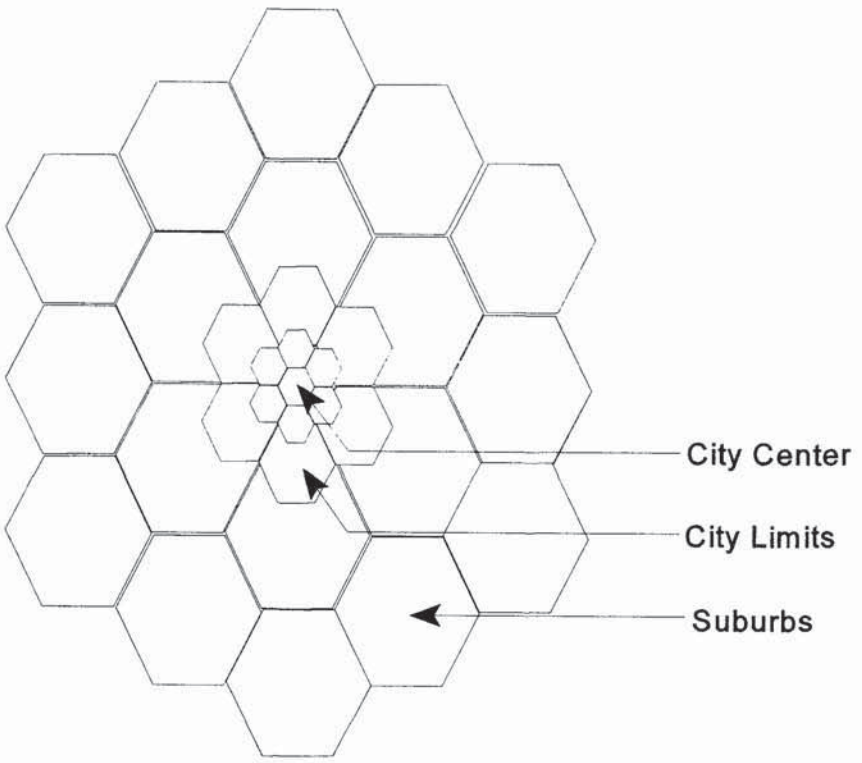


Figure 35. The cellular cartographer must remember that cellular implementation allows for varying cell sizes. The cell sizes generally become smaller as population density increases.

make an official map, you may wish to superimpose hexagons onto a road map of the area. Be sure to place the hexagons around the cell sites that you marked down during the visual inspection phase. Also keep in mind that cell sizes will vary. If you have enough data, you will have a good idea of the cell's relative size.

Targeting Mobile Units

I've read widely on cellular hacking, but I've yet to see anybody write about my favorite method of cellular interception. This method is so easy a blind iguana could do it.

Refer back to the FCC cellular frequency allocations earlier in this chapter. Note that mobile units transmit in the 824 to 849 MHz frequency range. If you're tailing an alleged drug dealer and he happens to place a cell call, you are obviously in no position to start mapping the area or tracking handoffs. A good detective already has the limit-search mode of his scanner preprogrammed for the mobile unit frequency range. At this point, you only need to turn your scanner on, press PROGRAM, LIMIT, and then the UP or DOWN search arrow. When you lock onto a nice, strong signal that does not fade as you drive along, chances are that you've found your subject's conversation. Better yet, you can look in his rearview mirror to see whether his lip movements match what you're hearing on the scanner. Be aware that mobile units also hand off, though less frequently. When this happens, just resume your limit-search until you reencounter the signal. If you are directly behind your subject, it might help to turn your squelch all the way up so that your scanner doesn't stop on unwanted signals. Also, make sure your DELAY function is set so that the scanner stays locked on the signal once you find it.

The foregoing drug scenario happened once on a surveillance gig. A goldmine was struck when the dealer said, "Okay, two o'clock. Second launch after the long dock." My being familiar with the area, this information was key. Sorry, Charlie.

Another beautiful thing about direct mobile monitoring is that many cellular service plans offer free nighttime and weekend use. This, combined with a flip phone's convenience, means that many folks use their cell phone on nights, weekends, and other off-peak hours in place of their regular phone.

Here's the scenario:

Your subject comes home after a long day's work, plops down on the couch, and realizes he forgot to make a call. He grits his teeth as he eyes the phone 20 feet away on the kitchen wall, but then the smile crosses his face. He pulls his cell phone out of his shirt pocket and begins making phone calls. Convenient. You know where your subject is, you know where his phone is. Where should you be? Outside his house scanning cellular mobile frequencies, that's where. An added benefit is that handoffs will not normally occur with a stationary mobile. A stationary mobile, by the way, is a 20th-century oxymoron meaning a mobile unit (e.g., flip phone) that is not moving (because your subject has plopped on his couch for the evening). In this case, a handoff will not occur unless some unusual interference is encountered in the neighborhood, such as another flip phone trying to use the same frequency or kids whipping crab apples at the radio tower.

As with most things, the simplicity of this method is not without compromise. The main disadvantage is that only one side of the conversation (the mobile) can be heard. One solution to this partially tenable situation is to have a couple of scanners going. While you're at it, throw in a couple of tape recorders. One scanner should be tuned into the subject's mobile unit with the output being recorded on one tape recorder. While that's being taken care of, you should be scanning cell sites with your other scanner looking for the two-sided version of the conversation. If you do your homework, you will have already figured out what cell site a mobile in your subject's neighborhood will be locked onto. If you go for the extra credit, the frequencies from this cell site will already be programmed into your scanner, right?

Tracking the Cops

Some time, when you have a warrant to investigate a corrupt police officer, listen over your scanner for dispatch to request that particular cop to "give me a landline" or "give me a 10-21." Both of these expressions mean "call me by phone." This is what police types do when they don't want a certain message going out over the radio. If you're lucky, the patrolman will have a cell phone. Since most cops like the comfort and safety of their cruiser, they will probably call dispatch via their cell phone as opposed to actually having to get out of their cozy cruiser and use an actual pay phone.

Tune into your local cell using any of the above methods and SCAN until you find your corrupt cop conversing with the dispatch officer. This can be fun if you're having an otherwise boring evening at home. You get to hear what kinds of things police types don't want going out over the radio. It's never what you'd expect. It's usually things like, "Your paranoid mother called again, and she swears that Elvis is standing in her driveway. She wants you to swing by the house." The cops don't want us to know that they're using taxpayer dough to handle personal matters. Sometimes, though, you can get a juicy tidbit. I won't spoil it for you by disclosing the details. Just get a warrant to monitor the cell calls of a corrupt cop and you'll hear plenty of goodies.

That'll Do Ya for Now

I have presented a lot of information about cellular phone system implementation, mapping, tracking, and hacking. If these topics are completely new to you, it may be best to reread this information later with a clear mind. Once you master these techniques, only a judge's signature stands between you and the wonderful world of cellular mapping and monitoring!

TUNING INTO BABY MONITORS

What if I said that you could show up at a surveillance gig only to find that a 1-watt crystal-controlled bug had already been successfully and unsuspectedly planted on the premises? This is what you have about 50 percent of the time these days if your subject happens to have at least one infant child. Young couples with children put these devices in their home and leave them on 24 hours a day for years at a time. A much smaller percentage then hire private detectives to spy on their spouses. If you target this market group, you may find yourself with some pretty easy to solve spy jobs!

Target This Market Group (See Above)

I wasn't kidding. After the crash of 1987, domestic spying jobs began to fall off, and my landlord at the time didn't seem to care when I explained this to him. This landlord was of the variety who preferred timely rental payments rather than good stories. So, I spent a day at the vital statistics registry looking through a four-year-old marriage index. I wrote down names and addresses of young couples who were from upper-class towns so I could be assured they'd have some money kicking around. I was also sure to stick with first-time marriages.

I spent the next day getting updated address information on these couples, because most move after getting married. One good resource for this is old marriage announcements. These announcements will usually tell you things such as when the wedding is to take place, where the couple will honeymoon, where they work, and where they plan to settle down and start fighting. Convenient. You can view old marriage announcements on microfiche at most libraries. Another good resource, more available today, is CD-ROM telephone databases. If you can't afford to buy one or don't have a computer with a CD-ROM drive, you can find these databases in larger libraries. The friendly librarian will even show you how to use the computer system and software.

Once you have compiled all of this information, send a tactfully worded advertisement to the wife explaining that you are a detective and available for domestic surveillance work.

hundred letters you send out. After a few weeks go by, send the same advertisement to the husbands of those wives who did not respond to your first mailing. Use a different envelope this time, though, so the wife, if she's the cheater, will not throw your ad in the circular file. You sent her the same envelope a few weeks ago, and she may recognize it. Women know their stationery, believe me! Be double sure to not send the ad to the husband(s) of any new clients you may have gotten from the first mailing!

You will usually get at least one nice-paying gig this way, and half the time you will already have a bug (the baby monitor) planted on the premises!

Some of you may be wondering why I chose to target first-time marriages of a four-year duration. Ever heard of the seven-year itch? Yeah, me too. Except scientific research shows that this "itch" occurs in humans on a four-year cycle, not seven. The "itch" is actually a biological instinct present in both sexes. Humans, after being in a monogamous relationship (i.e., marriage) for four years, instinctively begin to seek other potential mates. Some of us act on these instincts. Less mature individuals in first-time marriages are more likely to succumb to the four-year itch. Their hormonal urges are stronger, their sense of integrity is less defined, and, lacking any previous consequential experience, they are more willing to take the risk . . .

Adeste Infideles

Let's just say that I am acquainted with a certain married gentleman who believed, with good reason, that while he was out bringing home the bacon, his wife was home bringing in the beef—cake, that is. So one night he decided to put baby Daniel's crib in the master bedroom because the baby had been feverish the night before. At least, that's what my buddy, I mean casual acquaintance, told his beloved wife of four years.

The next morning while Daniel still lay sleeping in his crib, it was only prudent to innocently put the baby monitor on the nightstand by Daniel's crib while the couple cooked breakfast and got ready to start their day. My acquaintance carried the baby monitor's receiver around with him while he got ready for work, being sure his lovely wife noticed what a concerned father he was being. Before he left for the office he turned the receiver off and placed it in front of the baby monitor (which was "accidentally" left on), blocking the little red "power on" indicator light. The enterprising gentleman then kissed his unsuspecting wife good-bye and left for the day—or so he said.

Around 11:30 A.M. he returned from the office and parked in the back alleyway leading to the less fashionable side of his town house, where his wife was supposedly making the home. After a few minutes of listening to the rather convenient frequency of 49.830 MHz on his Radio Shack PRO-43 handheld scanner, he realized that his wife had confused "homemaking" with "making it at home"—with her best friend's husband, that is. I'll spare you the gory details . . .

How Often Does It Happen?

Okay, another example to balance out the sexes. I once had a surveillance gig for one rich lady who became curious about her husband's "painful back injury." Supposedly unable to work, he stayed home all day collecting worker's comp and watching the baby while she, a career woman, was out working. After billing my client for a two-hour interview at her office, I drove by the residence just to scope things out. Because it's the proper thing to do, I scanned baby monitor frequencies to see what I could glean from the neighborhood. To my surprise, I discovered a baby monitor in my client's residence. It seems that my client's husband, out of sheer laziness, had a baby monitor going all day long. What I heard coming over the baby monitor was enough to prove that my client's husband had anything but a painful back injury. Unless the phrase "painful back injury" can somehow be interpreted as "19-year-old mistress."

In this case my client got more than she bargained for. So did I. She kept me on for

nearly a month on a full-time basis without ever questioning my fees, expenses, or how I was able to record what was going on in her home while she was at work.

Tenant Tracking

If you own rental property, you know two things:

- No matter what a tenant writes on the rental application, you can't believe it. Even if all references check out, there are unscrupulous types out there who read books like *The Modern Identity Changer* just to get into an apartment.
- These tenants almost never replace the batteries in their smoke detectors. They tend to think it's the landlord's responsibility.

So what? Well, I'm not recommending this, but if you want to know what your tenants' real intentions are, a baby monitor PCB planted inside a smoke detector cover will get you the answer. Just make sure the smoke detector still works or you'll end up getting sued over that too. Oh yeah, be sure to get two warrants first: one for entering the apartment and one for planting the "bug."

Necessary Equipment

To tune into baby monitors you will need the following:

- A valid court-issued warrant
- A scanner that can receive the 48-49 MHz band, specifically,

  —49.830 MHz*
  —49.845 MHz
  —49.860 MHz
  —49.875 MHz*
  —49.890 MHz

* These seem to be the most popular ones, at least in my area (East Coast).

These frequencies are also used for cordless phone handsets, remote control cars, and kids' walkie-talkies. If you have a baby monitor, you can tune into other baby monitors by using the "parent unit." The parent unit is the little walkie-talkie type of receiver that comes with the baby monitor. If you shut your baby monitor off and leave the parent unit on, you may very well hear your neighbor making goofy sounds to a six-month-old or talking to the dog. If you drive through residential areas with the parent unit you will most definitely hear baby monitors. The signal will fade in and out fairly quickly as you drive past a house that has a baby monitor. The parent unit is not very sensitive. You may hear some interesting stuff, but a scanner will do you much better. A scanner with a 49-MHz antenna will do you even better than that. The parent unit, however, while not exactly a top-quality receiver, will suffice for a simple demonstration.

HACKING INTO ANSWERING MACHINES

Answering machines do not broadcast or otherwise transmit audio in real time, but they are still great surveillance gadgets. Think about it. If you have, or I should say, a police detective with a valid warrant has, the ability to dial undetected into someone's answering machine and retrieve messages left by careless confidants, then you have, or rather the police detective has, a means of gathering fun and useful information.

It's almost the year 2000, and I can't believe that I still know people who can't dial into their own answering machines, much less someone else's. Because of their ignorance, these people are probably the best targets for this type of spying. You may wish to keep this in mind next time your girlfriend, boyfriend, or business partner complains how "complicated" modern technology is.

The typical, modern-day, commercially available desktop answering machine has a numeric code used to access messages. Older models have a two-digit code and newer models have a three-digit code. Some antiquated models may have a one-digit access code.

There may be 50 ways to leave your lover, but there are only three ways to obtain an access code: If you have access to the machine you can look under the cover where the access code is usually imprinted, you can call the machine (preferably when the owner is not around) and hack away until you figure out the code, or you can monitor the phone line with a DTMF decoder (see Chapter 3) until the owner calls in and conveniently dials the access code into your scanner. Slick.

Hack, Hack, Hack

If you cannot otherwise obtain your subject's answering machine code, you must resort to hacking. Hacking means that you must call the machine directly and do some fancy guesswork to discover the code. It is imperative that you know that your subject is not home when you do this. How do you know your subject is not home? Well, if he doesn't answer the phone, then he's not home, right? WRONG! Never, ever, ever make the mistake of assuming this. Many people do not answer their phones these days. They let the machine do the work. Besides, if you're tracking the guy, it must be for a reason. If he's a deadbeat or avoiding the law, not answering the phone is most likely his standard operating procedure. So how do you know if your subject is not home? That's the job of the detective. You are the detective. Get it?

Older answering machines are easier to crack because there are only 100 possible combinations to try (00–99). Newer models with three-digit combinations are harder to crack, though still far from impossible.

The novice hacker will begin at 000 and proceed to 999 until the code is cracked. This is inadvisable. Especially since I personally know of at least one sick bastard who uses the code 999 just for the sake of pissing off novice hackers. The only message on the machine has been there for two years: "Hello, hacker, hope you didn't start at zero, zero, zero. Please dial the 20-digit secondary access code now—oh and I'll give you a clue—it's not a whole bunch of nines! BEEP!"

A better bet is to use your subject's personal information to your advantage. Typical codes people like to use are initials, birth dates, or names of children, grandchildren, lovers, and spouses. They also like to use other numbers or codes they already have, such as phone numbers, Social Security numbers, bank card codes, etc. Words representing hobbies and professions, such as DOC, ISKI, BEER, LAW, are also common pass codes. Finally, some people like to use sexually related words or numbers for codes, especially if they are young or immature.

If you don't know of any potential codes to try or if the ones you do know don't work, before submitting to a full hack from 000 to 999, try these strings of numbers:

- 012345678909876543210
- 000 111 222 333 444 555 666 777 888 999
- 696739969

These strings are good to try for a few reasons:

- They produce sequences that people are likely to use such as 111, 222, 123, 234, because they are easily remembered.
- There are some machines sold that are preprogrammed with simple default codes (00 and 000 are typical). The user is supposed to override this code with his own code after purchasing the machine. Many people don't know, don't care, or don't bother.
- There are some machines sold that default to a simple code (e.g., 00, 000, 999) if power is lost or if the backup battery dies. Many people forget to reset their code.
- The "739" sequence buried in the last string spells out "SEX" on the telephone keypad. People, especially young people, find that sexually related pass codes are easily remembered.

In most cases, the answering machine will not care whether you dial more than the expected number of digits. Some newer answering machines are hip to this and will say things like, "Sorry, please try again," after receiving three

digits. More sophisticated machines will hang up on you after a few incorrect tries. These types of machines are harder to crack because you need to keep calling back. This also increases your chances of being caught.

This sequence of numbers will crack any one- or two-digit answering machine code. For convenience, they are separated by spaces into groups of four.

- 0011 2233 4455 6677 8899 0987 6543 2102
- 2040 5060 7080 3130 4151 6171 8191 4246
- 5262 7282 9253 5736 3747 5838 4859 3949
- 9596 7976 4686 986

A Radio Shack Pocket Tone Dialer with 33-number memory will come in handy here. If you program these sequences into the tone dialer, you can play them back at rapid speed when trying to crack answering machine codes.

Programming a Tone Dialer for Easy Hacking

Procedure

1. Get a Radio Shack Tone Dialer (catalog item #43-146).
2. Slide ON/OFF switch to ON.
3. Slide DIAL/STORE switch to STORE.
4. Press MEMORY.
5. Press 0011 2233 4455 6677 8899 0987 6543 2102.
6. Press MEMORY.
7. Press 01.
8. Wait for the confirmation beep.
9. Press MEMORY.
10. Press 2040 5060 7080 3130 4151 6171 8191 4246.
11. Press MEMORY.
12. Press 02.
13. Wait for the confirmation beep.
14. Press MEMORY.
15. Press 5262 7282 9253 5736 3747 5838 4859 3949.
16. Press MEMORY.
17. Press 03.
18. Wait for the confirmation beep.
19. Press MEMORY.
20. Press 9596 7976 4686 986.
21. Press MEMORY.
22. Press 04.
23. Wait for the confirmation beep.
24. Slide DIAL/STORE switch to DIAL.
25. Test by pressing MEMORY 01.
26. You should hear the first string.

Using a Tone Dialer to Crack Answering Machine Codes

Procedure

1. Get a warrant.
2. Have a judge sign it.
3. When you're sure your subject's home is unoccupied, go to step 4.
4. Pick up your phone, wait for the dial tone, and then dial *67 to cancel Caller ID.[1]
5. Wait for the TelCo to make three short, clicky, dial tone sounds and then give you a new dial tone. You may now safely dial your subject's phone number.
6. Listen to your subject's greeting and memorize the pattern of beeps used to signal the end of the message.
7. Hang up without leaving a message.
8. Pick up your phone, wait for the dial tone, dial *67 to cancel Caller ID. (See note 1 below.)
9. Wait for the TelCo to make three short, clicky, dial tone sounds and then give you a new dial tone. You may now safely redial your subject's phone number.
10. Hold the Tone Dialer up to the phone's mouthpiece (the end into which you would normally speak).
11. As soon as the answering machine picks up, press the sequence MEMORY, 0, 1.
12. The first string will feed down the line.
13. If you successfully crack the code, you will

1. This step is crucial! If you have Caller ID permanently blocked, you may not need this step. For safety's sake, make double sure and dial *67 anyway. Please note that *67 only works for the call in which you dial it. You need to dial it every time you call your subject! If you hang up the phone before going to step 5, you must dial *67 again. Once you hang up the phone, *67 Caller ID blocking is canceled. Make sure you understand this step!

hear a tone or tones that sound different from the beep or beeps you memorized in step 6. If so, stop here and enjoy.

14. When you hear the end of the greeting, hang up immediately. Be especially sure you hang up before you hear the beep or beeps memorized in step 6.[2] If necessary, hit the PAUSE key on the Tone Dialer (when you call back, hit the PAUSE key again to resume where you left off).
15. Go to step 8 and try again beginning where you left off.[3]
16. Keep doing this until you've played memory locations 01–04.
17. If you are unsuccessful, try again. Make sure the Tone Dialer is held firmly to the mouthpiece. If you used PAUSE the first time, be sure to PAUSE in different places this time. It is possible that you paused in the middle of the correct code.

If this code-cracking method doesn't work after three tries, your subject probably has a pass code more than two digits long. You will need to commit to a full hack. The Tone Dialer will still come in handy for this, but the programming sequences will be considerably more involved. Expect to use all of your memory banks including P1, P2, and P3.

"Program my Tone Dialer for 1,000 possible three-digit combinations? But that's 3,000 digits! My Tone Dialer only holds 1,056 digits! You mean I have to buy three Tone Dialers?"

Well, if you carefully choose your code-cracking patterns, you will be able to get most, if not all, of the codes onto one Tone Dialer.

•		022	033	044	055	066	077	088	099	10
•	11	122	133	144	155	166	177	188	199	1
•	211	222	233	244	255	266	277	288	299	20
•	311	322	333	344	355	366	377	388	399	30
•	411	422	433	444	455	466	477	488	499	40
•	511	522	533	544	555	566	577	588	599	50
•	611	622	633	644	655	666	677	688	699	60
•	711	722	733	744	755	766	777	788	799	70
•	811	822	833	844	855	866	877	888	899	80
•	911	922	933	944	955	966	977	988	999	
•	100	200	300	400	500	600	700	800	900	
•	011	012	013	014	015	016	017	018	019	01
•	021	022	023	024	025	026	027	028	029	02
•	031	032	033	034	035	036	037	038	039	03
•	041	042	043	044	045	046	047	048	049	04
•	051	052	053	054	055	056	057	058	059	05
•	061	062	063	064	065	066	067	068	069	06
•	071	072	073	074	075	076	077	078	079	07
•	081	082	083	084	085	086	087	088	089	08
•	091	092	093	094	095	096	097	098	099	09

2. At this point, you must be sure no more tones are fed down the line. If tones get fed down the line after the machine begins recording, the owner of the machine will hear them upon checking his messages and become suspicious. If hacking manually, don't keep trying codes after the "beep."

3. At step 11 you will either have to press PAUSE to finish the previous memory location or move on to the code-cracking sequence stored in the next memory location (02, 03, 04).

For example, the 20 strings in the illustration on the previous page will give you 434 (43.4 percent) of the 1,000 (10^3) possible combinations while using little more than half the Tone Dialer's memory. Note that all of the strings still have room for more numbers at the beginning or end.

These 571 digits equal 434 three-digit combinations. Entered sequentially, this would have taken 1,302 digits. This method, therefore, is considerably more efficient. At this writing, I am devising a computer program that will calculate the most efficient method of programming a Tone Dialer for three-digit code cracking. As soon as the solution is available, I will post it on my Web site.

Other Features

Some machines do more than simply play back messages once you've cracked their code. Rewind, fast forward, and erase are among some of the other available options. Some machines even have the option of monitoring the room audio if you know the right code. These machines may present you with a menu, which is very convenient, but most do not. You have to know how the machine operates before you can use the options effectively. (If you happen to know the make and model of your subject's answering machine, you can order the literature from the manufacturer or get it from your local dealer. You can also buy the same machine and use it for a while until you learn how it works and then return it.) It's best not to "sort through" these options to learn the menu. Doing so may accidentally erase a message, which could give you away.

Most of these extra functions are useless, anyway. Fast forwarding and rewinding are not absolute necessities for the spy. If you have access to the messages, you should be recording them at your end anyway. In most cases, erasing messages can eventually lead to the spy's discovery. Sometimes, though, it can come in handy. For instance, if someone left the message, "Suzie, watch out. I heard Jack is stealing messages off your machine," then Jack may buy himself another day or two by erasing this message. Room monitoring, however, will most certainly come in handy if you can turn it on right before your subject comes home (so he doesn't hear the phone ring).

Don't Let This Happen to You

If you don't want any wise guys cracking your answering machine code, keep the greeting on your answering machine nice and short. "Hi. Leave a message," will do. By doing this, the would-be trickster does not have much time to send preprogrammed tones down the line before your machine starts recording them. Although this doesn't make it impossible for someone to steal your messages, it does make it much more difficult. And because the trickster will have to call back 30 times in a row to come up with 100 combinations, he is more exposed and you have a better chance of catching him in the act. If you have a three-digit security code, well then, that's even better.

You could also have no greeting at all on the machine and just let it beep as soon as it answers the call. Everybody knows what the beep means these days anyway. Go ahead, try it some time. You'll receive just as many messages from solicitors and nosy IRS types as ever before. But even this tactic won't work if you have a one-digit pass code. In this case, 10 calls max and they know your code. If you have this kind of answering machine, you have little hope for message privacy, and my suggestion is to smash it with a large brick and get a real answering machine.

The above security methods assume that anyone trying to crack your code is unwilling to let the attempt be recorded on tape. However, if the code cracker doesn't care or assumes that you're too stupid to know that DTMF tones left as a message means you're being hacked, he may just go ahead and speed-dial codes into your machine while being recorded. This will work and will crack your code. So if you ever come home only to find that someone has left a whole bunch of DTMF tones for a message, you can assume that someone is trying to crack (or has already cracked) your answering machine code.

Here's another thing to keep in mind. If you're like me and you have a "let the machine get it" attitude, you may just catch a code cracker in the act. This is why step 3 in the previous section asks you to make sure that your subject's home is unoccupied: you don't want to get caught this way! If you ever decide to "let the machine get it" and then hear a whole bunch of DTMF tones being left as a message, you can be pretty certain someone is trying to crack your code. If you hear your machine rewind before the end of the greeting and then click itself into play mode, someone has already stolen your code and is checking your messages. You must watch your machine for this action because most machines send the message audio over the phone line only. It is not audible in the room because the answering machine assumes nobody's there to hear it. If someone were there, they would have answered the phone, right? Well, we know better.

In the scenario depicted above, Caller ID can really come in handy. If you have Caller ID and the code cracker did not block it, you will readily know who the offending party is, and perhaps even pay him (or her?) a visit some foggy evening.

Hacking into Voice Mail

For our purposes, voice mail can mean company voice mail or the garden-variety voice mail services offered by your friendly local telephone company.

Voice mailboxes usually have at least a four-digit code, which is considerably more secure. The hacking method becomes difficult with voice mail, but a tenacious detective can still get the job done. Of course, try the obvious codes first (e.g., personal information, successive/consecutive numbers, sex words).

The most efficient way to get someone's voice mail pass code is to monitor his outgoing phone calls with a DTMF decoder (see Chapter 3). When the individual calls his office or the phone company to get voice mail messages, he will enter his pass code. This number will show up on your DTMF decoder. For best results, tape the call in case you miss anything. As always, remember to get that warrant first!

CHAPTER 6

PARTING THOUGHTS

I had to keep the "y" stuffed in my pocket because I'm really having "partying thoughts." It's been a long haul, my friends, and this old-fashioned spy needs to howl! My desk is a disaster area, and saying the same about my electronics bench would only be complimenting it. But I got the call from my editor today, and, with any luck, this puppy will be in the mail by noon tomorrow.

So, what's next?

Well, after a long vacation and getting caught up with my case load, I plan to design a PIC microcontroller module for the DTMF decoder we built. It will plug right into the BS1-IC interface port and add much more memory at less than one-third the cost. Look for it in *Popular Electronics*, on my Web site, and maybe even in a future book.

I'm also planning a pinhole video surveillance circuit and some audio and video wireless circuits based on the new miniature RF boards and chips that are now coming into fashion. As always, I'm open to comments, suggestions, and any circuit designs all'y'all may have.

I trust you have plenty to keep you busy for now. And if you feel so inclined, or perhaps even inspired, to waddle your way into the detective industry, be sure to leave your hit-or-miss database searches behind—we've enough pencil pushers and record chasers in this industry. Instead, bring a reliable bag of tricks—one that you've compiled through your own sweat and ingenuity. Where each circuit and method of implementation has been designed, tested, and refined by the very hand that puts it to use—the only hand that feeds you . . . the only hand you can trust . . . the hand belonging to one renegade member of a dying breed—*your* hand. The hand of an old-fashioned spy.

APPENDIX A

BIBLIOGRAPHY

The following were consulted while compiling this text. You may wish to check them out.

Cheek, Bill. *The Ultimate Scanner*. Boulder, CO: Paladin Press, 1995.

Chiaroscuro, Nick. *The Home Workshop Spy: Spookware for the Serious Hobbyist*. Boulder, CO: Paladin Press, 1997.

Headquarters, Department of the Army. *Basic Theory and Application of Transistors* (TM 11-690). Washington, D.C.: Superintendent of Documents, U.S. Government Printing Office, 17 March 1959.

Lapin, Lee. *Book II, How to Get Anything on Anybody*. San Mateo, CA: ISECO, Inc., 1991.

Larsen, Tom. *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians*. Boulder, CO: Paladin Press, 1997.

Lee, William C.Y. *Mobile Communications Engineering Theory and Applications*, Second Edition. New York: The McGraw-Hill Companies, Inc., 1998.

Mitel Corporation. *Analog/Digital TELECOM Components*, Issue 10, MT8870D/D-1. Ontario, Canada: Mitel Corporation, 1995.

Mitel Corporation. *Applications*, Issue 10, MSAN-108. Ontario, Canada: Mitel Corporation, 1995.

NRI Schools. *Electronics Training Courses*. Washington, D.C.: McGraw-Hill Continuing Education Center, 1981.

Radio Shack. "FM Wireless Microphone Cat. #28-4030," Instruction Sheet. Fort Worth, TX: Tandy Corporation, 1994.

Sharp Corporation. *Dot Matrix LCD Units with Built-In Controllers*. Osaka, Japan: Sharp Corporation, February 1987.

Uniden Corporation. *Betty Bearcat Frequency Directory*. Indianapolis, IN: Uniden Corporation of America, 1989.

APPENDIX B

LEGAL STUFF

The circuits, PCB designs, and schematics for all projects as well as the PBASIC program listing for the BS1 are the intellectual property of Sheldon X. Charrett, who is the copyright owner and may have applied for patent protection for certain circuit designs. When you purchased this book, you bought the right to use the designs and PBASIC program listing to build one corresponding project for your own use.

If you wish to use these circuit designs, PCB layouts, or the PBASIC program listing to develop products for sale to third parties, you must contact the author to discuss licensing arrangements (see Appendix C for information on contacting the author).

TRADEMARKS

The following is a list of registered names and trademarks that appeared in this book. The list is not intended to be complete.

Other company, brand, and product names mentioned in this book may be trademarks or registered trademarks of their respective holders.

TRADEMARK	OWNER
BASIC Stamp	Parallax, Inc.
Microsoft	Microsoft Corporation
Microsoft Works	Microsoft Corporation
Mitel	Mitel Corporation
Motorola	Motorola Corporation
Parallax	Parallax, Inc.
PBASIC	Parallax, Inc.
PIC	Microchip Technology, Inc.
Touch-Tone	AT&T Corporation
Word Perfect	Borland International
Word Perfect Draw	Borland International

APPENDIX D

FILES AVAILABLE

The following files are available at my Web site:

- All schematics, PCBs, and stuffing diagrams
- BS1 program listing
- Cellular layout spreadsheet in Microsoft Excel 97 format
- Microsoft Works database cellular charting and sorting routine

APPENDIX E

LISTING 1: FIRMWARE FOR LCD READOUT MODULE INTERFACED WITH DECODER MODULE*

```
' CONSTANTS
' ~~~~~~~~~
SYMBOL E       = 4     ' LCD enable pin (1 = enabled)
SYMBOL RS      = 5     ' Register Select (1 = char)
SYMBOL DV= pin6        ' Refers to I/O pin (P6) of LCD Module's IC1 (not pin 6 of IC)
SYMBOL MODE = pin7

' VARIABLES
 ~~~~~~~~~
SYMBOL outp    = B0        output workspace
SYMBOL char    = B1        char sent to LCD
SYMBOL address = B3
SYMBOL ctr     = B4

' LOAD THE EEPROM
' ~~~~~~~~~~~~~~~
'   **** SOFTWARE FIX ****
'   This allows for straight PCB Traces
    EEPROM ("D84#206B195A3*7C")

' Initialize the LCD (Hitatchi HD44780 controller)
' ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
LCD_INIT:
    Pins = %00000011    ' 8-bit mode
    dirs = %00111111    ' ~~~~~~~~~~

    PULSOUT E, 1
    PAUSE 5
    PULSOUT E, 1
    PULSOUT E, 1

    Pins = %00000010        ' 4-bit mode
    PULSOUT E, 1            ' ~~~~~~~~~~
```

```
char = %00101000        ' Dual line display / 5x7 font
GOSUB LCD_WRITE         '~~~
```

```
    GOSUB LCD_CONTROL
    ctr = 0                         ' Reset the counter

READOUT:
    address = address – 1           ' decrement the address
    read address, char              ' put data at address into char
    GOSUB LCD_WRITE                 ' write data at address to LCD
    PAUSE 250                       ' print out slowly for peace of mind
    ctr = ctr + 1                   ' increment counter
    GOSUB jump                      ' see if we need to jump to non-contiguous address space
    if MODE = 0 then START          ' see if user wants to exit
    if ctr = 16 then START          ' limit to one screen (there is still memory to play with)
    goto READOUT

LCD_CONTROL:
    LOW RS                          ' tell the LCD it's receiving a command
    GOSUB LCD_WRITE                 ' send the command
    HIGH RS                         ' put LCD back in data mode
    RETURN                          ' Return from subroutine

LCD_WRITE:                          ' Write char to LCD
    dirs = %11111111
    Pins = Pins & %00100000         ' RS = 1, data bus clear
    outp = char / 16                ' get high nibble
    Pins = Pins | outp              ' output the nibble
    PULSOUT E, 1                    ' strobe the Enable line
    Pins = Pins & %00100000         ' RS = 1, data bus clear
    outp = char & %00001111         ' get low nibble
    Pins = Pins | outp              ' output the nibble
    PULSOUT E, 1                    ' strobe the Enable line
    dirs = %00110000                ' Reset Pin Directions
    RETURN                          ' Return from subroutine

WrEEPROM:                           ' Write Character to EEPROM:
    address = address - 1
    WRITE address, char
    if ctr = 16 then LCD_INIT
    RETURN                          ' Return from subroutine

JUMP:                               ' Rectify Hitachi's addressing scheme
    IF ctr <> 8 then skip           ' Rectify P-BASIC's IF command
    char = %11000000                ' 192 in decimal (second 1/2 of LCD)
    gosub LCD_CONTROL               ' Nested RETURN is no problem here
    RETURN                          ' Return to address stored by GOSUB
    skip:
    RETURN                          ' Return to address stored by GOSUB
```

APPENDIX F

GLOSSARY

21.6 MHz—A common image frequency in FM signals.

900 KHz—A common image frequency in FM signals.

all'y'all—Plural of y'all. All of you all. Everybody. Often used by psychotic detectives.

base—The part of a cordless phone that is plugged into the wall. It is also known as a transponder and broadcasts both sides of a conversation.

BCD—Binary coded decimal.

cell—Where the feds put me after I wrote this book. The area covered by a cell site.

cell site—An antenna system implemented to broadcast to and receive transmissions from a mobile unit or flip phone.

commercial FM band—Nirvana, Pearl Jam, maybe even Styx but definitely NOT Yoko Ono. The area of the frequency spectrum from 88–108 MHz where commercial FM radio stations operate.

consorts—An overamplified rhythmic ceremonial ritual where performing musicians attempt to get more buzzed than their audience. Or the friends and associates of an operative's subject.

cordless phone—A home telephone system consisting of a base (see above), which is plugged into the wall, and a handset that uses radio signals in place of wires.

detective—A high-ranking police officer. A person licensed to investigate the habits and whereabouts of others. The guy standing behind you.

DIP—Dual inline package.

DTMF—Dual-tone multiplexed frequency. A system of encoding telephone company signals.

DV—Data valid, such as the data valid pin of Mitel's 8870 chip. It's easy to remember: you'd rather have DV than VD. Okay?

Faraday shielding—A type of shielding that attenuates electromagnetic transmissions.

FM—Frequency modulation. A method used to encode a carrier frequency with an audio frequency. Title of a Steely Dan song.

fundamental frequency—Equal to the carrier frequency. It is the frequency from which harmonics are generated.

GTa—Guard time absent. (See discussion of 8870 chip in Chapter 3.)

GTp—Guard time present. (See discussion of 8870 chip in Chapter 3.)

handset—The part of a cordless phone you walk around with.

harmonic—An RF image inherent in and harmonically related to the fundamental frequency. Sometimes harmonics can be picked up on a scanner if the signal is strong enough or close enough.

IC—Integrated circuit.

image—A radio frequency, not harmonically related to the carrier frequency, which can be picked up by a scanner.

LCD—Liquid crystal display. I took a lot of this stuff in the 1960s. No, wait—that was LSD.

LED—Light-emitting diode.

limit-search—A special scanning routine that most scanners are capable of. The routine allows you to scan between two preset frequencies: high and low.

listening post—A place from which surveillance is conducted.
LP—Listening post.
LSB—Least significant bit. In the binary number 0001 the "1" is the least significant bit because it is the right-most bit.
mobile—The part of a cellular phone system carried by the user, such as a flip phone.
MSB—Most significant bit. In the binary number 1000 the "1" is the most significant bit because it is the left-most bit.
operative—Person conducting a surveillance.
PCB trace—The metal strip on a printed circuit board that runs between two or more solder pads and acts as a conductor.
PEP—Peak envelope power.
phreak—Person who hacks into phone systems.
phreak show—Place where phreaks meet and share information and discoveries.
phreaked out—Someone obsessed with phreaking.
phreaking—The act of hacking a phone system.
red boxer—A sparring partner with a bad sunburn. Or a person who makes free calls from a pay phone.
repeat—To retransmit an RF signal.
repeater—A transmitter set up to retransmit RF signals, usually from a weaker transmitter, such as a ham radio or room bug.
ring—One part of a twisted pair.
roam—To move between cells in a cellular system or to be outside of your cellular service area. An ancient city in Italy.
scanner—A radio receiver capable of tuning to and scanning between many frequencies.
subject—A person under surveillance. A part of speech that usually precedes the predicate.
tape out—A port used to output audio to a tape recorder often found on larger, base-type scanners.
tip—One half of a twisted pair.
Touch-Tone—An AT&T trademark describing DTMF tones.
twisted pair—A couple of my old college buddies. Or a set of wires on which a phone service is installed, made up of the tip and ring.
varactor—A special diode with a known capacitance that changes as current passes through it.
zener diode—A silicon semiconductor device used especially as a voltage regulator.
zulu—Police code for the letter "Z." Another excuse to have a "Z" entry in this glossary.

APPENDIX G

PARTS SOURCES

SOURCES FOR 8870 DTMF DECODER CHIP

Celeritous Technical Services
5109 82nd St. #7, Suite 1200
Lubbock, TX 79424
E-mail: sales@celeritous.com
Web: www.celeritous.com
Contact: Allen Litton

Celeritous Technical Services Corporation (CTS) is the best source for this part. It uses state-of-the-art computer-aided engineering (CAE) tools and ASIC technology to create quick, quality, cost-effective form, fit, and function replacements for discontinued digital ICs. It serves official equipment manufacturers (OEMs) and distributors worldwide. I strongly suggest visiting its Web site—interesting stuff. CTS also makes kits. They have a copy of the parts list for all modules in the DTMF decoder series. When you call, ask them for a current quote if you're interested in a kit.

Tri-Group
326 Ilimano Street
Kailua, HI 96734
Web: www.surpluspage.com
E-mail: smokey@lava.net
Contact: J. Carter "Smokey" Thompson
or Rob Edgar

Spectrum Electronics, Inc.
1226 Bridge St. NW
Grand Rapids, MI 49504-5039
Web: www.SpectrumElectronic.com
E-mail: Spectrum_Electronics@csi.com
Contact: Gary Fisher

Any of the above companies may make kits or PCBs available if demand is sufficient. If you want a kit or PCB, please be sure to express your interest.

GENERAL PARTS SOURCES

Digi-Key
701 Brooks Ave. S.
P.O. Box 677
Thief River Falls, MN 56701-0677
Web: www.digikey.com

This is a good source for parts but otherwise very bureaucratic. Expect no help from the sales staff unless you've got a big order. And don't bother asking one of its employees to do a detailed cross-reference. Basically, you're on your own. Order the catalog, fill out the order form, and fax it or mail it back. Digi-Key's one saving grace is that all orders of $25 and up are shipped free.

JDR Microdevices
1850 S. 10th St.
San Jose, CA 95112-4108

JDR has a much reader-friendlier catalog than Digi-Key. It's done in color, often provides pin-outs, and is actually fun to read. Its biggest fault: $6.99 shipping charge for a 1-pound item. Avoid JDR if at all possible.